

JULIAN ASSANGE
 Jacob Appelbaum
 Andy Müller-Maguhn
 Jérémie Zimmermann

CYPHERPUNKS
 Libertatea și
 viitorul internetului

Colecție coordonată de
 CRISTIAN PÎRVULESCU

POLIS

Jacob Appelbaum
Andy Müller-Maguhn
Jérémie Zimmermann

Libertatea și viitorul internetului

Colecție coordonată de
CRISTIAN PÎRVULESCU

POLIS

JULIAN ASSANGE

Jacob Appelbaum • Andy Müller-Maguhn • Jérémie Zimmermann

CYPHERPUNKS

Libertatea și viitorul internetului

Julian Assange este redactorul-șef al WikiLeaks, distins cu premiul „Noile Media“ al Amnesty International (2009), premiul fundației Sydney pentru pace (2011), premiul „Walkley“ pentru jurnalism (2011) și premiul „Martha Gellhorn“ (2011). Unul dintre colaboratorii inițiali la lista de e-mailuri cypherpunk, este creatorul a numeroase proiecte de software inspirate de filosofia cypherpunk, inclusiv al sistemului de fișiere Rubberhose pentru criptare și al codului original pentru WikiLeaks. A mai publicat cartea *Underground* (împreună cu Suelette Dreyfus, 2012), o istorie a mișcării internaționale a hackerilor.

JULIAN ASSANGE

Jacob Appelbaum

Andy Müller-Maguhn

Jérémie Zimmermann

CYPHERPUNKS

Libertatea și
viitorul internetului

POLIS

Traducere din limba engleză de

VLADIMIR LAZURCA

Prefață la ediția în limba română de

CLAUDIU CRĂCIUN



Cyberpunks.
Freedom and the future of the Internet
Julian Assange împreună cu Jacob Appelbaum,
Andy Müller-Maguhn și Jérémie Zimmermann

Copyright © 2012 Julian Assange
Ediție publicată prin înțelegere cu OR Books LLC, New York



Editura Litera
O.P. 53; C.P. 212, sector 4, București, România
tel. 021 319 6390; 031 425 1619; 0752 548 372
e-mail: comenzi@litera.ro

Ne puteți vizita pe



Cyberpunks. Libertatea și viitorul internetului
Julian Assange

Copyright © 2016 Grup Media Litera
pentru versiunea în limba română
Toate drepturile rezervate

Editor: Vidrașcu și fiii
Redactori: Carmen Ștefania Neacșu, Mihaela Moroșanu
Copertă: Flori Zahiu
Tehnoredactare și prepress: Anca Suciu

Descrierea CIP a Bibliotecii Naționale a României
ASSANGE, JULIAN

Cyberpunks. Libertatea și viitorul internetului / Julian Assange;
trad.: Vladimir Lazurca – București: Litera, 2016

ISBN 978-606-33-0610-5

I. Lazurca, Vladimir (trad.)

Cuprins

Prefață la ediția în limba română (Claudiu Crăciun).....	7
Ce este un <i>cypherpunk</i> ?	29
Introducere:	
O chemare sub armele criptografice	31
Participantii la discuție	37
Nota editorului	40
Notă despre diversele încercări de a persecuta WikiLeaks și pe cei asociați ei.....	41
Intensificarea comunicării <i>versus</i> intensificarea supravegherii.....	49
Militarizarea spațiului cibernetic	61
Combaterea supravegherii totale cu ajutorul legilor omului	69
Spionajul sectorului privat	79
Combaterea supravegherii totale cu legile fizicii.....	87
Internetul și politica.....	95

Internetul și economia	113
Cenzura	137
Confidențialitate pentru cei slabi, transparență pentru cei puternici	163
Șobolanii de la Operă	171
Note	183

Prefață la ediția în limba română*

Numele lui Julian Assange nu este foarte cunoscut în România. Al par-tenerilor lui de dialog, cu atât mai puțin. Doar cei interesați de politica internațională, de dezvoltarea tehnologiei informației sau de drepturile fundamentale sunt familiarizați cu persoana sa și cu odiseea lui legală. Dar incomparabil mai mulți cunosc și chiar folosesc platformele și tehnologiile pe care Assange și colegii lui le analizează critic în cartea de față. Google, Facebook, Twitter, Amazon, Microsoft, Apple. Sunt companiile din avangarda tehnologiei informației și cele care au pre-luat internetul, îl structurează și, odată cu el, comunicațiile tuturor. Pe lângă faptul că sunt branduri influente, au putere economică, juridică și politică, iar aceasta crește exponențial. Cooperează cu guvernele, formând un complex tehnologico-informațional care deține controlul asupra interacțiunilor dintre miliarde de oameni. Perspectiva este amețitoare: miliarde de oameni angrenați în comunicare și schimburi și care produc urme vizibile și stocabile; întreaga istorie a umanității, de la cea individuală la cea macrosocială, se reflectă în uriașe centre de date. Iar de acolo, companiile private și guvernele extrag informații despre oricine și despre toți, devenind proprietarele unui tezaur de cunoaștere care le oferă o putere și o independență unice în istorie.

Problema fundamentală a internetului, cel puțin așa cum o văd Assange și colegii lui, este faptul că o întreagă civilizație s-a mutat în virtual, iar acest spațiu, din cauza tehnologiei de supraveghere, devine unul distopic, din care nu mai putem refuza să facem parte, dar asupra căruia nu mai exercităm nici un control. Avem de ales între a ne izola,

* Le sunt recunoscător lui Constantin Vică, Daniel Cernat și Nicoletei Andreescu pentru comentariile și sugestiile asupra textului.

refuzând participarea la interacțiunea socială, și a ne preda sfera privată și datele companiilor și guvernelor. Cypherpunks ne prezintă acest spectru, neliniștitor în întregul lui, cu scopul de a ghida o participare conștientă, responsabilă, protejată și descentralizată la spațiul virtual.

Volumul redă de fapt un dialog între membrii unei comunități mult mai largi și redutabile de specialiști în tehnologia informației, activiști, jurnaliști și analiști ai internetului. Scopul lor asumat este limitarea puterii companiilor și guvernelor, dezvăluirea secretelor de interes public și protejarea intimității din ce în ce mai fragile a cetățenilor, prizonieri benevoli ai internetului. Dialogul lor, dens și viu, nu este însă unul tehnic, un schimb între specialiști ai hardware-ului și ai software-ului. Este unul în care istoria, geografia, ideile, puterea și politica se întrepătrund cu tehnologia. Exact această întrepătrundere și interdependență fac dialogul semnificativ. Tehnologia nu constituie o sferă izolată, ci este inclusă în societate, transformând-o la fiecare pas. Direcțiile transformării pot fi problematice, pentru că orice tehnologie poate fi folosită și în scop constructiv, și în scop distructiv. Această ambivalență este prezentă și în acest caz. Astfel, a privi răspândirea tehnologiei informației ca fiind ceva inerent bun este un optimism care poate înșela. Tehnologiile nu produc în mod automat bunăstare, siguranță, sănătate, democrație și egalitate, mai ales atunci când se află în posesia unui grup restrâns sau când devin arme în mâinile unor organizații ori guverne. Tehnologia este parte a puterii, pe care o constituie și o conservă. Iar puterea exclude și include, divide sau unește, distruge sau construiește, favorizează sau discriminează.

Tiparul și cartea scrisă, mijloacele moderne de transport, electricitatea, telefonía, radioul și televiziunea au schimbat cursul istoriei. Efectele internetului asupra civilizației sunt la fel de puternice ca ale acestor tehnologii, dar, spre deosebire de acestea, care au avansat modular, inegal și într-un timp îndelungat, internetul cuprinde întreaga omenire într-un ritm extrem de rapid. Dialogul dintre cei patru autori arată că tehnologia informației și comunicațiilor schimbă tot – felul în care interacționăm și chiar cel în care percepem realitatea. Numărul celor care dețin dispozitive pentru conectarea la internet e în creștere exponențială. Telefoanele devin din ce în ce mai sofisticate, preluând funcțiile PC-urilor. Cu ajutorul dispozitivelor electronice

și al internetului, de la cele mai fragede vârste oamenii se informează, se educă, comunică, se distrează, cumpără și vând, își găsesc parteneri, își evaluează sănătatea, caută mijloace de transport, controlează aplicații și aparatele electrocasnice. Așa-numitul Internet al lucrurilor crește conectivitatea cu tot ceea ce ne înconjoară și ne este de folos. În fiecare zi devenim tot mai conectați și mai dependenți de tehnologie și internet. Iar această conectare lasă urme, arătând unde suntem, cu cine suntem, ce consumăm, ce ne place și ce nu ne place, ce stil de viață avem, cât de sănătoși sau de mobili suntem, cât de populari sau deprimați suntem. Fiecare aspect al vieții noastre, fiecare alegere, fiecare gest lasă o urmă digitală, stocată undeva. Prin simplul fapt că existăm digital, producem informație și devenim o țintă pentru cei interesați de respectivele informații. Interesul este economic pentru companii și politic pentru guverne. Împreună, acestea colaborează pentru a produce, stoca și analiza mai bine datele existenței noastre. Programele de supraveghere și spionaj se banalizează, înregistrarea comunicațiilor la fel. Programele de recunoaștere a vocii și a trăsăturilor faciale devin din ce în ce mai performante. Pare că vocația inovației tehnologice actuale este creșterea „lizibilității” comportamentului uman în toate aspectele acestuia. Iar această citire și ordonarea comportamentului uman individual devin imperativul guvernării și al economiei.

Protecția datelor personale și a comunicațiilor private este în principiu garantată constituțional, cel puțin în democrațiile liberale. Există o cultură a protejării datelor cu caracter personal, mai ales în Europa și în America de Nord, unde orice intruziune trebuie justificată și validată legal, și numai în relație cu o faptă ilegală în privința căreia există dovezi anterioare. Adică cei cărora li se ascultă telefoanele sau cărora li se citește poșta electronică sunt persoane care au comis sau urmează să comită o infracțiune. Limitarea drepturilor poate fi în principiu justificată, iar aceste limitări sunt prevăzute în legislație și validate de un judecător, independent de activitatea organelor de anchetă. Aceste proceduri au fost însă cu totul depășite de viteza cu care se dezvoltă tehnologia și de libertatea de facto pe care serviciile de informații și cele polițienești au căpătat-o inclusiv în democrațiile occidentale. Modelul dominant a devenit cel în care toate comunicațiile sunt supravegheate și înregistrate în masă, și abia apoi analizate de diferite agenții pentru a afla informații

relevante despre anumite persoane și grupuri (ceea ce Julian Assange numește interceptare strategică).

Stat, tehnologie și supraveghere

Contemplăm astăzi lumea nouă a comunicării și accesului la informații și putem avea iluzia unui sentiment de libertate. Idealiștii internetului timpuriu îl vedeau ca pe un instrument al cunoașterii și educației, liber și autogovernat, lipsit de obstacole și coerciție. Istoria recentă l-a dus însă în alte direcții. În primul rând, marile corporații au ajuns să îl domine. În al doilea rând, statele și-au extins monopolul asupra constrângerii și în acest spațiu, folosind acest monopol pentru a-și consolida puterea în lumea reală. Să devină oare internetul, dintr-o utopie a cunoașterii, un coșmar al profitului și supravegherii? Cei care au participat la acest dialog, și nu numai ei, asta cred. Este important să vedem cum s-a ajuns aici.

Statul a fost și a rămas principalul motor al dezvoltării tehnologice. Fără sprijinul lui direct, principalele realizări tehnologice moderne nu s-ar fi putut răspândi. Statul a construit căi ferate și le-a folosit pentru transport, comerț și război. A construit rețele electrice, drumuri și autostrăzi. Atunci când tehnologiile trebuiau transferate în infrastructuri fizice, statul era acolo, prin investiții, aprobări, legiferare, control, impozitare, servicii de urgență. Există o prezență variabilă, dar puternică a statului în operarea tuturor infrastructurilor, iar cele de importanță majoră sunt direct controlate de acesta. Tehnologia comunicațiilor și internetul au însă o traiectorie diferită. Spre deosebire de alte domenii, statul nu mai este, în aceste cazuri, motor al dezvoltării și/sau proprietar al infrastructurilor. Acestea sunt private. Terminalele și dispozitivele, cablurile de rețea, centrele de date, capacitățile de stocare sunt private. Expertiza umană este concentrată masiv în zona privată. Acest lucru pune statele într-o poziție dificilă în raport cu alte situații istorice, în care relația de autoritate era clară. De asemenea, pune companiile private într-o postură delicată, pentru că în principiu au datoria să își protejeze clienții¹. În practică, relația funcționează mult mai bine decât se poate anticipa. În țările autoritare, precum China, nu se poate pune problema protejării informațiilor private. Probabil nici în țări cvasiautoritare

precum Rusia. Relația este însă mai interesantă în SUA, care sunt singura superputere globală și, în același timp, țara cu cei mai puternici jucători pe piața serviciilor și produselor online. Fuziunea dintre interesele, resursele și viziunea marilor giganți ai internetului și guvernul american pare completă². Guvernul are acces direct la tot ce trece prin serverele acestor giganți, așa cum a dezvăluit contractorul NSA Edward Snowden³. Șefii marilor corporații sunt activi în diplomația economică și culturală americană⁴. Aceste corporații, dincolo de profiturile uriașe pe care le extrag, răspândesc în lume idei, valori și simboluri ce legitimează poziția dominantă a Statelor Unite în lume.

Puterea statală a fost întotdeauna suspicioasă cu supușii și ulterior cetățenii săi. Un bun conducător, un regim politic responsabil trebuie să știe ce gândesc și fac membrii comunității. Dar unde se află granița dintre guvernarea binevoitoare și luminată și controlul asupra societății? Democratizarea presupune creșterea controlului cetățenesc asupra puterii politice. În același timp, statul își dezvoltă infrastructura guvernării, care este folosită atât pentru administrare, cât și pentru control. Supravegherea guvernamentală, cel puțin în Europa, are o istorie lungă. Multă vreme, un stat eficient a fost acela care știa exact unde îi locuiau cetățenii, ce fel de proprietăți aveau, ce fel de activități economice întreprindeau⁵ – pentru a-i impozita sau trimite la război. Cu timpul, instituțiile polițienești, judiciare și carcerale s-au întărit, atât în democrații, cât și în regimurile despotice și autoritare⁶. Supravegherea în lipsa tehnologiilor actuale fiind o activitate costisitoare și intensă, în trecut aparatele polițienești trebuiau să se bazeze pe informatori și delațiune, pe un aparat birocratic masiv care să întrețină un sistem de strângere, arhivare și analiză a informațiilor. Pe rând, toate mijloacele de comunicare au fost interceptate – poșta fizică, transmisiunile radio, conversațiile telefonice. Chiar înainte de apariția internetului, statele erau prin urmare capabile să supravegheze la scară extinsă. Vârful acestei tendințe de monitorizare și control a fost statul totalitar, cel care, pe lângă ingineria socială violentă, a avansat cel mai departe în controlul total asupra indivizilor. Doar limitele tehnologice au împiedicat statele să reușească supravegherea deplină.

Arhitectura politică a supravegherii a fost concepută în timpul Războiului Rece, iar monitorizarea internetului astăzi este o extensie

a acesteia într-un nou spațiu. În primul rând, supravegherea este considerată o tactică de război, deci o chestiune de siguranță națională, justificând militarizarea și generalizarea acesteia. În al doilea rând, supravegherea este în mod egal ținută asupra adversarului și a propriilor cetățeni, aceștia din urmă fiind cu toții suspectați că nu ar fi loiali regimului, ci unei forțe străine. În al treilea rând, supravegherea trebuie să fie globală, pentru că războiul este la fel. Nici o națiune și nici un cetățean ai lumii nu se pot extrage din acest război. Statele Unite ale Americii și Uniunea Sovietică au concurat în aceeași logică, aparatele lor de spionaj și supraveghere răspândindu-se peste tot în lume, dar fiind în cele din urmă orientate cu precădere către interiorul respectivelor state. Ascultarea telefoanelor, urmărirea, interceptarea conversațiilor din anii 1950 și 1960 din America sunt un exemplu. Ulterior, SUA și-au dezvoltat sisteme de supraveghere sofisticate. Uniunea Sovietică, un stat autoritar, și-a dezvoltat la rândul său infrastructura de supraveghere pentru identificarea disidenților și menținerea regimului politic. Ca și în cursa tehnologică de război propriu-zisă, Statele Unite au avut și aici un avans tehnologic clar.

Sfârșitul Războiului Rece a detensionat parțial situația, dar nu a schimbat-o fundamental. Dezarmarea care a urmat a ținut arsenalul nuclear și pe cel convențional, și nu infrastructura de comunicații, respectiv de supraveghere. La zece ani de la sfârșitul Războiului Rece a apărut însă un nou tip de conflict, cel cu terorismul islamist, ca răspuns la atentatele asupra turnurilor gemene din New York și a Pentagonului din 2001⁷. Din nou, vorbim despre o problemă globală ce are ramificații în interior, deci supravegherea trebuie să îi urmeze. Transferul gândirii de tip Război Rece către noua amenințare s-a petrecut rapid. Rusia, de asemenea, a făcut transferul după atentatele de la Moscova (2002) și Beslan (2004). Rivalitatea geopolitică a părut pentru moment amorțită și înlocuită de lupta comună antiteroristă. Europa a făcut la rândul ei acest transfer, dar cu rezerve, chiar dacă se confruntase anterior cu incidente teroriste serioase, separatist-naționaliste sau ideologice. Însă atentatele de la Madrid (2004) și de la Londra (2005) și, recent, cele de la Paris (noiembrie 2015) și Bruxelles (aprilie 2016) par că o împing către militarizarea acestui conflict și susținerea supravegherii extinse pe care o presupune⁸.

Perioada post-Război Rece coincide cu răspândirea internetului. Monitorizarea și militarizarea lui erau doar o chestiune de timp. Prin faptul că cetățenii îl folosesc în mod voluntar, se rezolvă o mare și persistentă problemă a statelor. Informația devine disponibilă imediat ce deschizi un program de navigare pe web sau apelezi pe cineva de pe telefonul mobil. Ceea ce părea cândva o imposibilitate devine acum realitate. Iar acest proiect nu este nici măcar un secret. Programul Total Information Awareness (TIA) își propune nici mai mult, nici mai puțin decât supravegherea totală. Datorită creșterii capacităților de stocare, este posibil ca un asemenea proiect să fie susținut de bugetul unei singure țări, în cazul de față SUA. Globalizarea părea că le-a răpit statelor din autonomie și le-a limitat setul de instrumente pe care îl au la dispoziție. Contrar acestei perspective, cel puțin în domeniul securității și al informației, datorită inerției, războaielor și internetului, ele devin, dimpotrivă, și mai puternice.

Internetul și democrația

Impactul tehnologiei asupra procesului guvernării este major. Acest lucru este valabil atât pentru țările democratice și pentru cele nedemocratice, cât și pentru cele în tranziție de la o categorie la cealaltă. Tehnologia informației și internetul devin factori de accelerare sau de temperare a unor tendințe istorice, fie că ne referim la transferul ideilor revoluționare de la o societate la alta, fie la mobilizarea sau reprimarea mișcărilor de opoziție. În dialogul din volum, tema democrației și a democratizării este tratată pasager, perspectiva dominantă fiind aceea că tipul de regim nu contează, atât democrațiile, cât și non-democrațiile fiind structural asemănătoare, având un fel de ADN comun, bazat pe penetrarea totală a sferei private și pe controlul interacțiunilor sociale mediate digital. În plus, se desprinde imaginea unor Leviatani, state concurente sau aliate care își dispută puterea la nivel global, dar a căror trăsătură comună este controlul cvasitotal asupra propriilor cetățeni. În această lume nouă democrația nu există, fiind transformată într-un joc electoral superficial, la vârful unei piramide a puterii în care blocurile

sunt constituite din servicii de informații, birocrății opace și corporații puternice, cele care gestionează datele tuturor.

Este o imagine total contrastantă față de cea triumfalistă a victoriei democrației liberale asupra tuturor celorlalte forme de guvernare, răspândită după încheierea Războiului Rece. De asemenea, este o imagine total contrastantă față de cea a internetului și a tehnologiei informației ca principali aliați ai mișcărilor de opoziție ce luptă pentru democratizare. De ce unele state se democratizează și altele nu, de ce unele democrații rezistă și altele nu, care sunt factorii și mecanismele ce favorizează democrația sunt întrebări care preocupă știința politică. Fără a detalia răspunsurile posibile, foarte numeroase și deseori contradictorii, ne putem rezuma la o definiție minimală a democratizării drept proces istoric de constrângere și limitare a puterii politice prin intermediul legilor, al instituțiilor reprezentative și al participării electorale extinse. Astfel, puterea politică este legitimă, inclusiv sub aspectul utilizării coerciției, numai dacă este investită de către cetățeni prin vot și numai dacă procesul alegerii și al guvernării propriu-zise se supune unor reguli constituționale care trasează clar limitele puterii și responsabilității. În modernitate, acest proces a presupus centralizarea puterii de către principii și apoi limitarea puterii acestora de către birocrății publice și adunări parlamentare alese în mod direct. Mecanismele ce fac democrația să funcționeze sunt cele prin care drepturile și libertățile individuale sunt protejate, participarea politică a cetățenilor este încurajată, câștigarea și pierderea puterii se fac în mod pașnic, prin alegeri, iar puterea, în momentul în care este câștigată, nu este folosită împotriva opoziției sau a grupurilor minoritare. Firul roșu al tuturor acestor mecanisme și proceduri democratice este unul simplu: numai cei aleși în mod direct pot conduce o societate democratică. Acolo unde societatea este condusă de către persoane care nu au fost alese prin vot, precum regii sau principii, sau de către persoane făcând parte din corpuri speciale precum clerul sau armata, nu poate fi vorba despre o democrație. Democrația reprezintă o stare de echilibru între instituții și grupuri sociale, deseori fragil, inclusiv în cadrul a ceea ce numim democrații consolidate. Cel mai frecvent dezechilibru – și cel mai important – este cel dintre stat și societate. Atunci când asimetria de putere dintre acestea crește, democrația e în pericol.

Ce impact au tehnologia informației și internetul asupra regimurilor autoritare? Aparent, le slăbesc, așa cum am văzut în cazul Primăverii Arabe, când internetul a fost indispensabil mobilizării opoziției. Internetul are un rol antemergător important – cu ajutorul său circulă idei, argumente și simboluri care pot eroda susținerea regimurilor autoritare. Importanța internetului este relevată și de atenția pe care o acordă autoritățile limitării accesului și cenzurii. Resurse importante sunt dedicate acestor activități. În cazurile în care mișcările de opoziție nu reușesc îndepărtarea regimului autoritar respectiv, folosirea internetului are efectul invers, de slăbire a opoziției. Acest lucru se întâmplă pentru că opoziții își dezvăluie public pozițiile și tacticile și devin ținte ale represiunii. Așadar, internetul poate fi un instrument eficient al opoziției, dar numai în măsura în care aceasta este foarte puternică, iar regimul autoritar, prea slab pentru a organiza represiunea. Tehnologia și informația ajută, dar nu pot transforma structura socială și raporturile de putere existente, cel puțin pe termen scurt. Dacă nu există o anumită configurație de forțe, interne și externe, contestarea și îndepărtarea regimurilor autoritare nu pot avea loc. Iar dacă acestea reușesc să își construiască infrastructura necesară supravegherii totale, schimbarea de regim devine foarte dificilă.

Tehnologia informației și internetul funcționează ca acceleratori ai tendințelor autoritare, mai ales atunci când societatea respectivă este confruntată cu un dușman extern sau intern, real sau imaginat. Regimurile autoritare au inclusă în structura lor nevoia de dușmani, necesari pentru a putea menține unitatea în timpuri de criză sau atunci când performanțele regimului nu îi asigură acestuia legitimarea populară. Dușmanii interni iau forma unor minorități religioase, etnice sau lingvistice, a mișcărilor de opoziție, a organizațiilor nonguvernamentale sau a mass-mediei. Dușmanii externi sunt vecini sau puteri regionale ori globale. Supravegherea extinsă este justificată prin nevoia de a cunoaște și combate inamicii ordinii și unității naționale. În cazul în care unele dintre grupuri aleg calea rezistenței armate, situația este definită ca un război și tratată ca atare. Mai mult, regimurile autoritare realizează un transfer. Grupurile de opoziție, oricare ar fi natura opoziției acestora, sunt tratate ca un întreg, și instrumentele de represiune sunt transferate de la un grup la altul, de obicei de la cel mai periculos și violent către

cele mai pașnice. Retorica, supravegherea, intimidarea, represiunea sunt folosite și împotriva luptătorilor, dacă există, și împotriva opoziției politice pașnice. Ca exemplu, guvernul turc condus de Recep Tayyip Erdoğan amestecă opoziția politică, presa și grupările armate, folosind lupta antiteroristă ca justificare pentru represiunea tuturor grupurilor de opoziție.

În schimb, relația dintre tehnologia informației, internet și democrații pare complementară. Datorită internetului, cetățenii devin mai bine informați, interacționează mai ușor, inclusiv din punct de vedere politic⁹. Internetul este noua locație a dezbaterii publice, indispensabilă oricărei forme de democrație. Guvernarea poate deveni mai transparentă prin facilitarea accesului la informații publice. Forme de scrutin electronic sunt experimentate peste tot în lume. Cu toate acestea, construcția unei infrastructuri care face comportamentul individual și interacțiunile de grup perfect vizibile este de natură să afecteze structural democrația. Acest lucru se întâmplă în primul rând prin modificarea comportamentului individual, prin internalizarea unei autocenzuri care subminează participarea și contestarea. În al doilea rând, se întâmplă prin penetrarea grupurilor active din societate și prin creșterea capacității de intervenție asupra lor. Nu în ultimul rând, prin dezechilibrarea serioasă a raporturilor de putere dintre cei aleși democratic și cei care nu au fost aleși. Infrastructura de supraveghere nu este controlată efectiv de nici un oficial ales, fapt valabil inclusiv în democrații solide precum Suedia sau Franța.

Pentru unii, înregistrarea și stocarea datelor nu reprezintă o problemă, ei preluând argumentul: „Nu fac nimic ilegal și în consecință nu am de ce să mă tem”. Dar ar trebui să fie conștienți că, de îndată ce sunt stocate undeva, aceste date pot fi extrase, fără ca ei să mai poată avea nici un control asupra lor. În orice moment, elemente care țin de viața personală pot fi accesate, pentru că ești ținta supravegherii guvernamentale. Iar această supraveghere este realizată nu pentru că s-a făcut ceva ilegal, ci pentru că persoana ar putea fi problematică din punct de vedere politic. Experiențele de hărțuire și intimidare guvernamentală prin care au trecut cei care participă la dialogul din volum sunt edificatoare. Dacă faci parte dintr-un ONG care militează împotriva unor proiecte guvernamentale sau dacă ești jurnalist de investigație, dacă faci parte

dintr-un partid politic, de opoziție sau de la guvernare, dacă participi la proteste sau semnezi petiții publice, toate acestea te pot aduce în atenția celor care monitorizează. Există foarte puține garanții că acest lucru nu ți se poate întâmpla și ție. Tehnologia de supraveghere, stocarea și folosirea datelor sunt controlate de funcționari și experți care lucrează într-un regim strict de confidențialitate și care raportează unor responsabili militari ce sunt într-o foarte mică măsură răspunzători în fața conducătorilor politici aleși. Astfel, cunoașterea totală este mai accesibilă regimurilor autoritare decât celor democratice, dar în măsură egală posibilă și tentantă, căci infrastructura supravegherii îi acordă puterii politice o autonomie față de societate căreia cu greu i se poate rezista.

Strategii ale rezistenței

Având în vedere mobilizarea extraordinară a guvernelor și marilor corporații în direcția digitalizării și a supravegherii, se pune problema fundamentală a posibilității de a rezista. Rezistența este cu atât mai dificilă, cu cât viteza cu care întreaga lume se mută în spațiul virtual este mai mare. Absența din virtual poate însemna izolare, vulnerabilitate și precaritate. Știm însă că instituțiile politice se transformă pentru a supraviețui, iar odată cu acestea regimurile juridice. Știm de asemenea că toate instituțiile politice și tipurile de guvernare au fost contestate de-a lungul timpului. Dar de data aceasta nu discutăm despre un regim, guvern sau ideologie anume, ci despre un *modus operandi* statal care se generalizează indiferent de forma de organizare politică. În volum se discută pe larg despre strategiile de rezistență posibile. Cele două strategii discutate și comparate explicit sunt folosirea „legilor omului“, adică a instituțiilor politice și juridice, pentru limitarea supravegherii, respectiv folosirea „legilor fizicii ale informaticii“, adică a tehnologiei de anonimizare și de criptare a comunicațiilor. Mai adăugăm o strategie de altfel utilizată și perfecționată de WikiLeaks, și anume dezvăluirea activităților guvernării prin scurgerea de date relevante către public¹⁰. Recentele scurgeri de date de la o companie panameză specializată în operațiuni financiare arată că nu numai guvernarea este vulnerabilă,

ci și companiile, mai ales acelea care au făcut din secret și anonimitate un produs¹¹. Nu în ultimul rând, se discută calea transformării culturale, prin care cetățenii să fie făcuți conștienți de răspândirea supravegherii, să fie educați în a folosi instrumente de protejare a datelor private și în a participa la viața virtuală în multiple rețele și grupuri ce rezistă masificării și centralizării internetului.

Pot funcționa mecanismele democratice și juridice în direcția protecției vieții personale? Până în acest moment, se pare că prea puțin. Inclusiv în țările cu regimuri democratice considerate solide, instituțiile reprezentative – parlamentele – au dificultăți majore în a controla executivile și în principal ramurile militare și de informații ale acestora. Prin agitarea spectrului războiului și al feluritelor tipuri de amenințări, are loc o dezvoltare rapidă a infrastructurii digitale și de supraveghere, slab înțeleasă în funcționarea ei efectivă și foarte slab contestată politic în cadrele electorale și democratice. Cu toate acestea, cel puțin în spațiul nord-atlantic, au existat victorii importante care arată că presiunea mediatică, publică și civică poate da rezultate. În Statele Unite, președintele Bill Clinton s-a opus operaționalizării de către Pentagon a două sisteme paralele – Total Information Awareness (TIA) și The Mother of All Data Bases (Mama tuturor bazelor de date) –, un refuz ce pare a reflecta mai mult o luptă politică internă în care NSA a reușit să oprească două proiecte pe care nu le controla, și mai puțin un efect al presiunii publice¹². Lupta juridică poate de asemenea să funcționeze. În 2015, pe 6 octombrie, Curtea Europeană de Justiție a invalidat acordul dintre Statele Unite și Uniunea Europeană numit „Safe Harbour”, acord prin care se permitea marilor corporații americane să transfere și să stocheze în Statele Unite datele personale ale cetățenilor europeni¹³. Această invalidare se datorează unui tânăr austriac, Maximillian Schrems, care a făcut o plângere împotriva autorităților naționale irlandeze, care permiteau transferul de date de pe serverele aflate în Irlanda către cele aflate în Statele Unite, unde nu beneficiau de o protecție suficientă. În volum se discută și despre lobby-ul eficient realizat de către autorii *Cypherpunks* în fața Parlamentului European, lobby care împreună cu presiunea publică de pe tot continentul au dus la suspendarea acordului ACTA¹⁴. În Europa, curțile constituționale se află deseori în prima linie de apărare a libertăților individuale și a datelor personale. Rețele

de ONG-uri și de activiști sunt permanent mobilizate pentru a opri tentativele guvernelor și corporațiilor de a extinde monitorizarea, conform principiului „anonimitate pentru cei slabi, transparență pentru cei puternici“.

A doua strategie, cea a utilizării „legilor fizicii“, este una ponderent tehnică. Așa cum guvernele și corporațiile se află într-o permanentă „cursă a înarmărilor“ în privința capacităților de supraveghere, în mod similar cetățenii și societatea civilă trebuie să se angreneze într-o cursă de dezvoltare a capacităților de criptare care să o anuleze pe prima. Generalizarea soluțiilor de criptare pare o soluție ideală, ce va permite în același timp utilizarea internetului și o oarecare protecție, niciodată completă, a datelor personale. Criptarea ajută în depășirea inconvenientului de a nu fi proprietar *de facto* al nici uneia dintre părți fizice ale internetului – dispozitive, cabluri, centre de date. Eficiența acestei metode este probată, paradoxal, tot de către guverne și corporații în cursa pentru securitate și supremație. Guvernele și-au perfecționat metodele de criptare pentru a nu fi vulnerabile în fața adversarilor. De ce nu ar folosi și cetățenii aceleași instrumente pentru a se proteja de guverne?¹⁵ Folosirea soluțiilor de criptare nu va elibera internetul, ci va duce la o împărțire a acestuia, având de-o parte giganții privați conectați cu guvernele și de cealaltă o mulțime de comunități și de rețele autonome care își construiesc spații libere de interacțiune. Aceste rețele și grupuri nu sunt doar culturale sau economice, ele au o semnificație profund politică, căci participă la o reconstrucție a democrației, una de la bază, orizontală și autonomă, ca alternativă la democrația formală, centralizată politic și tehnologic, în care libertatea este compromisă odată cu distrugerea sferei private.¹⁶ Aceste spații le vor fi însă accesibile numai celor care reușesc să stăpânească tehnologia. Astfel, o parte din elita high-tech se va transforma și în avangardă a luptei democratice, o nouă disidență care se va opune unei „structuri extrem de restrictive, omogenizate, postmoderne, transnaționale și totalitare de o complexitate de necrezut, absurdă și devalorizată“ (Julian Assange).

Care va fi soarta încercărilor de a crește transparența activității guvernelor, atât în ceea ce privește politica externă și purtarea războaielor, cât și în ce privește activitatea de supraveghere? Ele probabil

vor continua, inspirate de WikiLeaks sau de exemplul lui Edward Snowden. Edward Snowden, fost angajat al unei companii private care subcontracta servicii de la Agenția americană Națională de Securitate, a fost printre primii care au dezvăluit, cu informații din interior, existența uriașului complex de supraveghere pe care îl întrețin SUA și aliații săi occidentali. Virulența atacurilor asupra lui Snowden se explică prin faptul că pune guvernarea într-o situație delicată, imposibil de legitimat din punct de vedere democratic. Dezvăluirile lui Snowden transformă ceea ce părea o sursă de putere într-o sursă de vulnerabilitate. Existența unui instrument ideal de supraveghere și control devine o vulnerabilitate majoră, de data aceasta de tip politic și democratic. Cum mai pot avea încredere cetățenii, oricât de dispuși ar fi, într-un guvern care îi spionează permanent? Spectrul terorismului și al criminalității cibernetice pare să nu fie de ajuns pentru a justifica o intruziune de o asemenea magnitudine în viața privată a acestora. Ceea ce au aflat guvernele odată cu dezvăluirile mediatizate global ale WikiLeaks-ului și ale lui Snowden este că la rândul lor pot fi monitorizate și supravegheate, că la rândul lor, ca și cetățenii, produc date și lasă urme digitale. Și că, în principiu, pot fi trase la răspundere pentru asta.

România. De la totalitarismul ideologic la totalitarismul digital

Unde se află România pe această hartă globală a informației și supravegherii? Istoria ei recentă, echilibrul precar dintre instituții și chiar poziția geografică o transformă, din păcate, într-o candidată ideală pentru accesul în distopia controlului social. Într-o perioadă foarte scurtă a făcut tranziția de la totalitarismul ideologic comunist la totalitarismul digital, preluând atât moștenirea supravegherii comuniste, cât și tendințele globale ale supravegherii dezvoltate după Războiul Rece. Ceea ce a facilitat acest proces este slăbirea instituțiilor reprezentativ-democratice, care au reușit doar într-o mică măsură să se impună în fața executivului și în special a serviciilor de informații. Digitalul și online-ul sunt terenurile în care democrația românească își testează viabilitatea și forța. Pentru moment, ceea ce ar fi trebuit să facă partidele

și Parlamentul, și anume a apăra drepturile fundamentale și viața privată, este *de facto* delegat societății civile, presei și instituțiilor care încă rezistă presiunilor, de exemplu Curtea Constituțională.

În anul 1989 România era o țară izolată, condusă cu o mână de fier de un cuplu prezidențial, o elită de partid și un aparat polițienesc masiv, Securitatea. După ce se îndepărtase atât de Uniunea Sovietică, cât și de țările occidentale, regimul politic avea toate motivele să creadă că se afla în pericol. Baza socială se clătina, așa cum arătase Brașovul în 1987, tehnocrația economică nu mai dădea rezultate, iar birocrăția de partid obosise. În aceste condiții, supraviețuirea regimului depindea de succesul intimidării și al represiei, care la rândul lor depindeau de abilitatea Securității de a urmări cetățenii. Practicile de violare a corespondenței, ascultare ambientală și ascultare a telefoanelor se banalizaseră. Cenzura oficială era dublată de o eficientă autocenzură a comportamentului individual. În cele din urmă, operațiunea masivă de interceptare și ascultare a dat greș, lanțul evenimentelor din decembrie 1989 petrecându-se prea rapid pentru ca supravegherea să mai conteze. După căderea comunismului, procesul de lustrare nu a demarat convingător, iar aparatul de partid și cel de Securitate și-au continuat existența în noile cadre democratice. Au urmat niște ani tensionați și confuzi în care practicile de supraveghere masivă au fost limitate, deși nu a fost clar dacă tehnica și personalul au dispărut.

Integrarea euroatlantică, scop declarat al României în tranziția sa timpurie, a presupus și reforma sectorului militar și de informații. Ideea controlului civil asupra acestora era o condiționalitate a NATO, iar această condiționalitate a impulsionat procesul de reformă pentru care presiunile publică și politică interne erau prea slabe. Armata a trecut printr-un proces mai transparent de reformă, care a presupus atât eliminarea serviciului militar obligatoriu, cât și reducerea semnificativă a personalului și capacităților de luptă. Reforma serviciilor de informații, în mod expres cerută de partenerii nord-atlantici, a fost mult mai discretă și lipsită de vigoare, dar cu un impact mare asupra politicii și a economiei. Dacă relațiile elitei civile cu Armata nu fuseseră problematice nici măcar în comunism, cele cu serviciile secrete erau mai complicate. În timp se construiseră niște instituții mult mai puternice și mult mai autonome decât cele ale Armatei. Iar pericolul pentru

tânăra democrație românească era mult mai mare. Reforma serviciilor a presupus pensionarea sau ieșirea din sistem a unui număr important de foști angajați. Mulți au intrat în afaceri, construind o zonă gri, în care se acționează prin aparenta respectarea a legilor pieței, dar în care se păstrează legături puternice cu instituțiile pe care, în principiu aceștia le-au părăsit. Poate nu întâmplător, unele dintre ramurile economice cel mai serios penetrate de aceste grupări au fost cele de telecomunicații și IT. În paralel s-a continuat reconfigurarea rolului instituțional al serviciilor secrete. Schimbarea majoră a intervenit în 2004, odată cu alegerea unui nou președinte. Șocul atentatelor de la New York a produs nu doar teamă, ci și o reconfigurare a ținutelor și metodelor de lucru. Lupta antiteroristă, configurată pe modelul american, a început să fie exportată peste tot în lume. Această luptă, așa cum am arătat anterior, întărește și mai mult statul în raport cu cetățenii, în special în ceea ce privește supravegherea. România, deja parte a NATO, deși nu avea o problemă teroristă pe teritoriul țării, a transferat și adaptat modelul. Pentru serviciile secrete din România, dar nu numai, acest lucru a fost o gură de aer proaspăt, fiindu-le astfel reconfigurate rolul și legitimitatea. În noul cadru, acestea nu mai reprezintă instituțiile care au ajutat regimul comunist, ci o parte importantă a luptei globale împotriva terorismului, deci pentru libertate și democrație.

În al doilea rând, și acest lucru este valabil în special pentru serviciile secrete românești, ele au fost instrumentalizate în lupta anticorupție, identificată drept amenințare la adresa securității naționale. Acest diagnostic e acceptat și susținut de o mare parte a opiniei publice. Comparativ cu lupta antiteroristă, cea anticorupție are un mare avantaj din perspectiva creșterii influenței serviciilor și a generalizării supravegherii. Dacă „teroristul” este pentru cetățeni o prezență rară, exotică și neclară, „coruptul” este o prezență familiară și răspândită în toate straturile societății. Un „dușman” intern ideal, a cărui urmărire presupune accesul oriunde, de la instituții publice și până la tribunale, spitale și școli. Cele două justificări ale supravegherii au mers în paralel, punctate permanent în spațiul public de către reprezentanții formali și informal ai serviciilor secrete. Războiul civil din Siria, izbucnirea unui scurt război civil în Ucraina, criza refugiaților, atentatele din noiembrie 2015 din Franța și cele din

aprilie 2016 din Belgia, toate au fost folosite pentru a sublinia nevoia de stabilitate și securitate, narațiunea principală a instituțiilor de forță.

În această configurație în care instituțiile democratice par că au pierdut controlul asupra serviciilor de informații, cât de răspândită este supravegherea?¹⁷ Este extinsă și se va extinde în continuare. Ca orice al cetățean al lumii care folosește serviciile unor giganți ai internetului și tehnologiei, cetățeanul român are datele reținute și stocate undeva. Nu este foarte clar ce date și informații sunt puse la dispoziția serviciilor din România, atât de către marile companii, cât și de către guvernul american. Într-o anumită măsură, nici nu contează, atât timp cât aceste instituții sunt conectate direct la serverele providerilor de servicii de internet și de comunicații mobile. Instituția care gestionează activitatea de interceptare este SRI, prin Centrul Național de Interceptare a Comunicațiilor (CNIC), iar entitatea respectivă a acționat într-un vid legislativ în care nu era clar ce responsabilități și puteri are, în special în ceea ce privește protejarea drepturilor fundamentale și a datelor cu caracter personal. Vidul legislativ nu l-a împiedicat însă să opereze. Cifrele arată o creștere semnificativă de la an la an a mandatelor de interceptare¹⁸.

În luna martie 2016 însă, Curtea Constituțională a decis că interceptările realizate de către SRI nu pot fi acceptabile ca probe în instanță. Această decizie a transmis o undă de șoc, pentru că majoritatea dosarelor de corupție au fost instrumentate cu ajutorul tehnicii de interceptare a SRI, instituție ce are o situație de cvasimonopol asupra interceptărilor. Repoziționarea instituțiilor a fost rapidă. Consiliul Suprem de Apărare a Țării, un adevărat guvern paralel gestionat de către președinție, a propus schimbarea legislației prin ordonanță de urgență și astfel SRI a devenit organ special de cercetare penală, cu dreptul de a participa la instrumentarea dosarelor care țin de siguranța națională și terorism. Soluția găsită a fost criticată de societatea civilă ca fiind foarte probabil neconstituțională¹⁹. Mai mult, conform strategiei privind siguranța națională, aceasta este definită foarte extins²⁰. Astfel, există puține garanții instituționale și procedurale că temeiul siguranței naționale va fi invocat corect și proporțional. Prin aceeași ordonanță de urgență, CNIC este obligat să asiste organele de urmărire penală atunci când au un mandat de supraveghere tehnică dispus de instanțele de

judecată conform dispozițiilor Codului de procedură penală. Persistă însă neclaritățile de ordin legal și constituțional, precum și garanțiile că datele personale sunt protejate conform principiilor Cartei drepturilor fundamentale a Uniunii Europene²¹.

După atentatele din luna martie 2016 de la Bruxelles, în mod previzibil, s-a solicitat de către guvern și președinție rediscutarea și aprobarea în regim de urgență a așa-numitului pachet „Big Brother”, ce cuprinde prevederi privind siguranța cibernetică a României. De asemenea, prin declarații publice ale reprezentanților executivului și ai serviciilor de informații s-a încercat în mod neconvingător să se lege atentatele teroriste și conflictele din Orientul Mijlociu de folosirea cartelelor pre-pay din România, care în prezent pot fi cumpărate fără a fi nevoie de identificarea cumpărătorului. Obligatorietatea declarării identității este un alt obiectiv asumat de către serviciile de informații. Pachetul inițial „Big Brother” a fost analizat de Curtea Constituțională și declarat neconstituțional (Decizia Curții Constituționale nr. 17/2015). Societatea civilă a solicitat în mai multe rânduri dezbateri pe tema pachetului, a venit cu propuneri de amendare, dar acestea nu s-au concretizat²². Astfel, pare că s-a ajuns la un blocaj în care executivul, inclusiv președinția, invocă pericolul terorist, dar refuză dialogul cu societatea civilă și nu pare capabil să prezinte propuneri viabile din punct de vedere constituțional.

Instalarea Leviatanului digital în România este întâmpinată cu rezistență, în principal din partea societății civile, a opiniei publice, a unei mici părți a presei și a sectorului privat de comunicații și, foarte important, din partea Curții Constituționale. Ceea ce însă este oprit sau amânat ca demers legislativ se petrece deja în realitate. Comunicațiile unui număr foarte mare de cetățeni sunt supravegheate și stocate. Este posibil ca aceste comunicații să nu poată fi folosite în instanță, dar de cele mai multe ori nici nu este nevoie. Acestea se pot scurge către presă, așa cum s-a mai întâmplat, sau pot fi folosite ca instrumente de presiune și șantaj. Contextul internațional nu este favorabil protecției vieții private și a comunicațiilor, și țara noastră nu se poate extrage acestuia. Iar acest context este folosit pentru a extinde supravegherea, împărțită între diferite agenții guvernamentale străine și naționale, mari corporații și companii care oferă soluții de supraveghere. Mai devreme

sau mai târziu, în paralel cu rezistența civică și politică împotriva legalizării acesteia, e posibil să fie nevoie să ne alfabetizăm cu toții în folosirea sigură a internetului și a programelor. Dar numai dacă prețuim libertatea și protecția sferei private, două lucruri care au lipsit acestei societăți înainte de 1989 și de care ar fi trebuit să ne bucurăm odată cu tranziția la democrație.

Claudiu Crăciun

1. FBI-ul american a anunțat recent că a reușit să intre în telefonul Apple al unei persoane implicate într-un atac terorist fără ajutorul companiei, după ce aceasta a refuzat să asiste autoritățile. Accesarea datelor a fost posibilă cu ajutorul unei firme private.
2. Influența guvernamentală americană asupra politicii internetului pare să se diminueze, trecându-se către o guvernare internațională. ICANN, organismul care stabilește regulile de atribuire de nume de domenii Internet și de adrese IP, este supravegheat de un Comitet Consultativ Guvernamental din care fac parte toate statele lumii. Este notabilă și dezvoltarea Forumului Guvernanței Internetului, susținut de Organizația Națiunilor Unite.
3. Dezvăluirile lui Edward Snowden arată cât de extinsă este activitatea de supraveghere, acesta referindu-se și la convorbirile telefonice și mesajele text, nu exclusiv la internet. Monitorizarea țintește nu numai cetățenii ci și lideri politici de peste tot din lume, inclusiv din țările NATO, aliate ale SUA; vezi Glenn Greenwald (2015), *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Picador, și www.glenngreenwald.net.
4. Pentru o analiză mai detaliată, vezi Julian Assange (2014), *When Google Met WikiLeaks*, OR Books
5. Vezi James C. Scott (2007), *În numele statului. Modele eșuate de îmbunătățire a condiției umane*, Polirom
6. Vezi Michel Foucault (2005), *A supraveghere și a pedepsi*, Editura Paralela 45
7. Cei patru cavaleri ai Infoapocalipsei, cei pe care guvernele îi invocă pentru a extinde supravegherea, sunt, conform lui Julian Assange: terorismul, pornografia infantilă, spălarea banilor și traficul de droguri.
8. De exemplu, guvernul german a fost autorizat să instaleze programe de tip troian pentru accesarea comunicațiilor persoanelor suspecte; *German government to use Trojan spyware to monitor citizens*, Deutsche Welle, 22.02.2016: <http://www.dw.com/en/german-government-to-use-trojan-spyware-to-monitor-citizens/a-19066629> (accesat în data de 4 aprilie 2016).

9. „*Internet est devenu le système nerveux de nos sociétés*”, interviu luat de către Alexandre Lacroix lui Julian Assange, *Philosophie Magazine*, 30.05.2013: <http://www.philomag.com/lepoque/reportage/julian-assange-internet-est-devenu-le-systeme-nerveux-de-nos-societes-7525> (accesat în data de 4 aprilie 2016)
10. *Ce este WikiLeaks*, 3.11.2015: <https://wikileaks.org/What-is-WikiLeaks.html> (accesat în data de 4 aprilie 2016)
11. *Panama Papers: The secrets of dirty money*, Süddeutsche Zeitung: <http://panama-papers.sueddeutsche.de/en/> (accesat în data de 4 aprilie 2016)
12. Vezi dialogul lui Julian Assange cu Ignacio Ramonet în Ignacio Ramonet (2015), *L'Empire de la surveillance*, Galilee, pp. 147–149
13. Curtea de Justiție a Uniunii Europene, Luxemburg, 6.10.2015, Decizia C-362/14, Maximillian Schrems v Data Protection Commissioner: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf> (accesat în data de 4 aprilie 2016)
14. Campania a fost coordonată de organizația franceză La Quadrature du net. Mai multe informații despre campanie se pot găsi aici <http://www.laquadrature.net/en/acta> (accesat în data de 4 aprilie 2016).
15. O variantă interesantă este supravegherea de „jos în sus” de către cetățeni a autorităților (*sousveillance*), vezi David Bollier, *Sousveillance as a Response to Surveillance*, 24.11.2013: <http://bollier.org/blog/sousveillance-response-surveillance> (accesat în data de 4 aprilie 2016).
16. Eric Hughes (1993), *A Cypherpunk's Manifesto*: <http://www.activism.net/cypherpunk/manifesto.html> (accesat în data de 4 aprilie 2016)
17. Conform estimărilor, personalul de 12 000 de agenți secreți e depășit doar de al FBI. Cu o populație de 2,5% din totalul grupului de țări, România are mai mult de 15% din agenții grupului; în ceea ce privește proporția față de populație: există 60 de angajați în serviciile interne la sută de mii de locuitori. Următorul clasat, Polonia, are 13 angajați; bugetul SRI are cea mai mare pondere în cheltuielile publice: jumătate de procent, de cinci ori mai mult decât media celor 10 state, care este de o zecime de procent. FBI se descurcă cu doar o șeptime de procent din cheltuielile publice totale ale SUA. Și, în termeni absoluți, SRI reușește să cheltuiască mai mult decât serviciile omoloage din Germania, Franța, Italia sau Polonia. Estimările au fost realizate de Lucian Davidescu, *Cât de mare este SRI față de serviciile din alte țări*, 14.09.2014: <http://riscograma.ro/9129/cat-de-mare-este-sri-fata-de-serviciile-din-alte-tari/> (accesat în data de 4 aprilie 2016).
18. Din datele Rapoartelor anuale ale SRI se desprind următoarele cifre: 2005 – 6 370 de mandate, 2006 – 8 693 de mandate, 2007 – 10 272 de mandate, 2008 – 15 170 de mandate, 2009 – 22 176 de mandate; 2010 – 30 624 de mandate, 2011– 35 678 de mandate, 2012 – 36 085 de mandate, 2013 – 38 884 de mandate, Radu Tudor, *Interceptări: 600% creștere în ultimii 10 ani!*, 27.01.2015:

<http://radu-tudor.ro/interceptari-600-crestere-in-ultimii-10-ani/> (accesat în data de 4 aprilie 2016).

19. *Metodele speciale de supraveghere. Societatea civilă cere garanții legale privind respectarea drepturilor omului*, TVR, 31.03.2016: http://stiri.tvr.ro/metodele-speciale-de-supraveghere-societatea-civila-cere-garantii-legle-privind-respectarea-drepturilor-omului_72601.html (accesat în data de 6 aprilie 2016).
20. „Strategia reflectă necesitatea promovării unui concept de securitate națională extinsă – fundamentat pe democrația constituțională și respectul mutual dintre cetățeni și stat – care vizează interesele care converg spre asigurarea securității naționale, manifestate în următoarele domenii: apărare (înțeleasă în dublă calitate normativă, de apărare națională și apărare colectivă), ordine publică, activitatea de informații, contrainformații și de securitate, educație, sănătate, economic, energetic, financiar, mediu, infrastructuri critice”, *Strategia Națională de Apărare a Țării*: http://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf (accesat în data de 6 aprilie 2016).
21. Carta drepturilor fundamentale a Uniunii Europene, Articolul 8. Protecția datelor cu caracter personal: (1) Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc. (2) Asemenea date trebuie tratate în mod corect, în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege. Orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora. (3) Respectarea acestor norme se supune controlului unei autorități independente. <http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A12012P%2FTXT> (accesat în data de 6 aprilie 2016).
22. Vezi documentul Asociației pentru Tehnologie și Internet, susținut de alte șase ONG-uri, *Comentarii la propunerea de lege privind securitatea cibernetică*, APTI, 25.02.2015: <https://www.apti.ro/comentarii-proiect-lege-securitate-cibernetica-2016> (accesat în data de 2 aprilie 2016).

Ce este un *cypherpunk*?

Activiștii *cypherpunk* militează pentru folosirea criptografiei și a unor metode similare ei pentru a efectua schimbări de natură socială sau politică.¹ Fondată la începutul anilor '90, această mișcare a avut activitatea cea mai intensă în perioada „războaielor criptografice“ din anii '90 și în urma „primăverii internetului“ din 2011. Termenul de *cypherpunk*, derivat din (criptograficul) *cipher* și *punk*, a fost introdus în Oxford English Dictionary în 2006.²

Introducere:

O chemare sub armele criptografice

Această carte nu este un manifest. Nu mai este timp pentru așa ceva. Această carte este un avertisment.

Lumea nu alunecă pe nesimțite către o nouă distopie trans-națională, ci se îndreaptă spre ea cu pași repezi. Acest fenomen nu a fost suficient recunoscut în afara cercurilor de securitate națională. A fost ținut ascuns prin tănuire, complexitate și dimensiune. Internetul, cel mai valoros instrument de emancipare al nostru, a fost transformat în cel mai periculos mijlocitor al totalitarismului care a fost văzut vreodată. Internetul e o amenințare la adresa viitorului civilizației umane.

Aceste transformări au survenit pe tăcute, din cauză că cei care știu ce se întâmplă lucrează în industria supravegherii globale și nu au nici un motiv să vorbească deschis. Dacă e lăsată să continue pe această cale, civilizația globală va deveni în câțiva ani o distopie postmodernă a supravegherii, din care scăparea nu va fi posibilă decât pentru cei mai pricepuți dintre noi. De fapt, s-ar putea să se fi ajuns deja acolo.

Deși mulți scriitori au în vedere semnificația internetului pentru civilizația globală, ei se înșală. Se înșală pentru că nu au acel simț al perspectivei pe care-l oferă experiența directă. Se înșală pentru că nu s-au întâlnit niciodată cu inamicul.

Nici o descriere a lumii nu supraviețuiește primului contact cu inamicul.

Noi am întâlnit inamicul.

În ultimii șase ani [până la editarea acestui volum – 2012], WikiLeaks a intrat în conflict cu aproape fiecare stat puternic. Cunoaștem noul regim de supraveghere din interior, pentru că i-am aflat secretele. Îl cunoaștem dintr-o perspectivă a combatantului, pentru că a trebuit să ne protejăm oamenii, resursele financiare și informatorii. Îl cunoaștem dintr-o perspectivă globală, pentru că avem oameni, active și informații în aproape fiecare țară din lume. Îl cunoaștem dintr-o perspectivă temporală, pentru că luptăm împotriva acestui fenomen de ani de zile și l-am văzut dublându-se și răspândindu-se, iar și iar. Este un parazit cotropitor, ce se hrănește cu societățile care se conectează la internet. Se întinde pe întreaga planetă, infectând fiecare stat și popor în calea sa.

Ce este de făcut?

Odată ca niciodată, într-un loc care nu e nici aici, nici acolo, noi, creatorii și cetățenii tânărului internet, am discutat despre viitorul noii noastre lumi.

Am văzut că relațiile dintre oameni vor fi mediate de noua noastră lume și că natura statelor, care se definesc prin felul în care oamenii schimbă informații, valoare economică și forță, se va schimba și ea.

Am văzut că fuziunea dintre structurile statale existente și internet a creat posibilitatea schimbării naturii statelor.

În primul rând, amintiți-vă că statele sunt acele sisteme prin care curge forța coercitivă. Facțiunile din cadrul unui stat pot concura pentru susținere, lucru care duce la fenomene democratice de suprafață, dar la temelia statelor stau aplicarea, respectiv evitarea sistematică a violenței. Proprietatea asupra pământului, proprietățile, chiriile, dividendele, taxele, amenzile judiciare, cenzura,

drepturile de autor și mărcile comerciale sunt impuse prin amenințarea cu aplicarea violenței statale.

De cele mai multe ori nici nu suntem conștienți de cât de aproape suntem de violență, pentru că facem cu toții concesii pentru a o evita. Asemenea marinarilor care adulmecă briza mării, rareori ne oprim să reflectăm la întunericul pe care se sprijină lumea noastră de la suprafață.

Care va fi mijlocitorul forței coercitive în noul spațiu al internetului?

Are vreun sens să ne punem întrebarea aceasta? Există vreun loc pentru noțiunea de violență coercitivă în acest spațiu imaterial, acest tărâm platonice al ideilor și al fluxului de informații? O forță care poate să modifice arhivele istorice, să asculte telefoanele, să dezbine popoarele, să transforme complexitatea în dărâmături și să ridice ziduri, asemenea unui armate de ocupație?

Natura platonice a internetului, a fluxului de idei și informații, este coruptă de originile sale fizice. Bazele sale sunt cablurile cu fibră optică ce se desfășoară pe fundul oceanelor, sateliții care se învârt deasupra capetelor noastre, serverele adăpostite în clădirile din orașe ce se întind de la New York la Nairobi. Asemenea soldatului care l-a ucis pe Arhimede cu o simplă sabie, se poate întâmpla ca o miliție bine înarmată să pună mâna pe vârful dezvoltării civilizației occidentale, tărâmul nostru platonice.

Noua lume a internetului, separată de vechea lume a atomilor bruți, tânjea după independență. Dar statele și aliații lor și-au propus să controleze noua noastră lume – prin controlul substratului său fizic. Statul, asemenea unei armate în jurul unui puț de petrol sau unui agent vamal care caută să smulgă mită la frontieră, va învăța în scurt timp să se folosească de controlul pe care-l deține asupra spațiului fizic pentru a ajunge să controleze tărâmul nostru platonice. Va împiedica independența la care am visat pentru ca apoi, ghemuit lângă cablurile optice și în jurul

stațiilor de recepție la sol a informațiilor de la sateliți, să înceapă să intercepteze în masă fluxul de informații al noii noastre lumi – însăși esența sa – exact atunci când fiecare relație umană, economică sau politică va fi aderat la acesta. Statul se va infiltra în venele și arterele noilor noastre societăți, înhățând fiecare relație exprimată sau comunicată, fiecare pagină web citită, fiecare mesaj trimis și fiecare cuvânt căutat pe Google, iar apoi va stoca pentru totdeauna toate aceste lucruri știute de ea, miliarde de interceptări zilnice, o putere nemaivăzută, în uriașe depozite secrete. Va extrage fără încetare din această comoară, producția intelectuală privată a întregii omeniri, cu algoritmi de căutare sau de recunoaștere după tipar din ce în ce mai sofisticăți, îmbogățind comoara și mărinind la maximum discrepanța de putere dintre cei interceptați și cei care interceptează. Iar apoi, statul va folosi în lumea fizică ceea ce a aflat, pentru a declara războaie, pentru a dirija atacuri cu dronă, pentru a manipula comisiile ONU și tratatele comerciale și pentru a-și favoriza propria și vasta rețea de industrii, de prieteni și de persoane care cunosc dedesubturile.

Dar noi am descoperit ceva. Singura noastră speranță împotriva dominației totale. O speranță pe care, cu curaj, discernământ și solidaritate o vom putea folosi pentru a opune rezistență. O proprietate stranie a universului fizic în care trăim.

Universul crede în codare.

Este mai ușor să codezi o informație decât să o decodezi.

Am observat că putem folosi această stranie proprietate pentru a crea legile unei lumi noi. Pentru a separa noul nostru tărâm platonice de temeliile sale fizice, de sateliți, de cabluri oceanice și de cei care le controlează. Pentru a ne fortifica spațiul în spatele unei cortine criptografice. Pentru a crea tărâmurile noi, la care cei care controlează realitatea fizică nu au acces, fiindcă ar avea nevoie de resurse infinite ca să ne urmeze pe acele căi.

Și, astfel, pentru a ne declara independența.

Savanții din Proiectul Manhattan au descoperit că universul permite construcția bombei atomice. Aceasta nu era o concluzie evidentă. S-ar fi putut ca armele nucleare să nu se supună legilor fizice. Totuși, universul crede în bombe atomice și reactoare nucleare. Ele sunt un fenomen pe care universul îl binecuvântează, asemenea sării, mării sau stelelor.

La fel, universul, universul nostru fizic, are acea proprietate care face posibil ca un individ, sau un grup de indivizi, să cifreze un lucru într-un mod sigur, automat, chiar și fără să știe, în așa fel încât toate resursele și toată voința politică a celei mai mari superputeri din lume să nu-l poată descifra. Iar căile pe care cifrarea le formează între oameni se pot uni pentru a crea regiuni întregi eliberate de forța coercitivă a statului exterior. Eliberate de interceptarea în masă. Eliberate de controlul statal.

În acest fel, oamenii își vor putea opune propria voință voinței unei superputeri mobilizate și vor putea învinge. Criptarea este o întruchipare a legilor fizicii, iar ea nu ascultă de amenințările gălăgioase ale statelor, fie acestea și distopii transnaționale ale supravegherii.

Nu este un lucru evident că lumea trebuia să funcționeze în acest fel. Dar cumva universul privește criptarea cu bunăvoință.

Criptografia este forma supremă a acțiunii nonviolente directe.

Deși statele care dețin armament nuclear pot exercita o violență nelimitată chiar asupra a milioane de oameni, criptografia puternică face ca un stat, chiar folosindu-se de o violență nelimitată, să nu poată viola intenția indivizilor de a ține secrete față de el.

Criptografia puternică poate rezista unui uz nelimitat al violenței. O problemă de matematică nu va putea fi rezolvată niciodată prin forță coercitivă.

Dar am putea oare să luăm acest fenomen straniu al lumii noastre și să-l transformăm într-unul dintre blocurile fundamentale,

emancipatoare cu care să construim independența omenirii în tărâmul platonice al internetului? Iar pe măsură ce societățile se vor fi conectat la internet, vom putea reflecta acea libertate înapoi în realitatea fizică pentru a redefini statul?

Amintiți-vă că statele sunt sistemele care determină unde și cum se va aplica de regulă forța coercitivă.

Răspunsul la întrebarea câtă forță coercitivă din lumea fizică se poate infiltra în tărâmul platonice al internetului este dat de criptografie și de idealurile cypherpunk.

Pe măsură ce statele se conectează la internet și viitorul civilizației noastre devine una cu viitorul internetului, trebuie să redefinim relațiile de forță.

Dacă nu facem acest lucru, universalitatea internetului va transforma omenirea globală într-o rețea uriașă de supraveghere și control în masă.

Trebuie să dăm alarma. Această carte este strigătul în noapte al unui străjer.

În data de 20 martie 2012, aflându-mă în arest la domiciliu în Regatul Unit și așteptându-mi extrădarea, m-am întâlnit cu trei prieteni și camarazi de strajă cu gândul că, poate, vocile noastre la unison i-ar putea trezi pe locuitorii cetății. Trebuie să împărtășim ceea ce am aflat cât încă mai este o șansă ca tu, cititorule, să înțelegi și să reacționezi la ce se întâmplă.

A venit timpul să luăm în mână armele noii noastre lumi, să luptăm pentru noi înșine și pentru cei pe care-i iubim.

Sarcina noastră este să asigurăm autodeterminarea unde încă se mai poate, să oprim înaintarea distopiei acolo unde nu se mai poate, iar dacă orice altceva va eșua, să-i accelerăm autodistrugerea.

Julian Assange, Londra, octombrie 2012

Participanții la discuție

JULIAN ASSANGE este redactorul-șef și vizionarul din spatele WikiLeaks.³ Inițial un colaborator la lista de e-mailuri Cypherpunk, Julian este astăzi unul dintre exponenții cei mai proeminenți ai filosofiei cypherpunk din lume. Activitatea sa în cadrul WikiLeaks a conferit popularitate politică expresiei tradiționale a mișcării cypherpunk: „Confidențialitate pentru cei slabi, transparență pentru cei puternici“. În timp ce activitatea sa cea mai vizibilă presupune un exercițiu viguros al libertății de exprimare pentru a constrânge instituțiile puternice la transparență și pentru a le trage la răspundere, el este de asemenea un critic acerb al încălcării abuzive a confidențialității individuale de către stat și corporații. Julian este autorul a numeroase proiecte de software inspirate de filosofia cypherpunk, cum ar fi primul *port scanner* *strobe.c* pentru TCP/IP, sistemul de fișiere Rubberhose pentru cifrare negabilă* și codul original pentru WikiLeaks.⁴ În adolescență, Julian a fost unul dintre primii care au făcut cercetări în ceea ce privește confidențialitatea datelor computerelor și rețelelor, înainte ca unele tipuri de *hacking* să fie definite prin lege ca activități criminale. Devenit

* În engleză *deniable encryption*, un sistem de criptare ce permite negarea existenței unui mesaj sau fișier criptat din cauză că nu se poate dovedi existența acestuia. (n.tr.)

apoi activist și furnizor de internet în Australia în anii '90, Julian este de asemenea coautorul cărții *Underground*, scrisă împreună cu Suelette Dreyfus și care reprezintă o istorie a mișcării internaționale a hackerilor, carte care a inspirat în mare parte filmul *Underground: The Julian Assange Story*.⁵

JACOB APPELBAUM este unul dintre fondatorii comunității Noisebridge din San Francisco, membru al organizației Chaos Computer Club din Berlin și dezvoltator.⁶ Jacob este un partizan al Proiectului Tor și cercetător în cadrul acestuia – un sistem care garantează confidențialitatea online și care permite tuturor oamenilor să se opună supravegherii și să împiedice cenzura internetului.⁷ În ultimul deceniu, interesul său a fost să ajute activiștii pentru protecția mediului și drepturile omului. În acest sens a publicat cercetări inedite despre securitate, confidențialitate și anonimitate într-o mulțime de domenii de cercetare, de la expertiza informatică la marijuana în scop medical. Jacob este de părere că fiecare are dreptul să citească liber, fără restricții, și dreptul să se exprime liber, fără excepții. În anul 2010, când Julian nu a putut ține o conferință în New York, Jacob a ținut-o în locul său. De atunci el, prietenii săi și familia sa au fost hărțuiți de către guvernul Statelor Unite: interogați la aeroporturi, supuși unor perchezițiuni intruzive și amenințați de către reprezentanți ai legii cu viitoare agresiuni sexuale în închisoare; i-a fost confiscat echipamentul, iar activitatea online i-a fost supusă unei somații secrete. Jacob nu se lasă însă intimidat de aceste măsuri, continuă să lupte în procesele juridice aflate în desfășurare și rămâne un apărător declarat al libertății de exprimare și un susținător zelos al WikiLeaks.

ANDY MÜLLER-MAGUHN este membru veteran al Chaos Computer Club din Germania, fost membru al consiliului său de conducere și purtător de cuvânt.⁸ Este unul dintre cofondatorii EDRI, European Digital Rights, un ONG care militează

pentru respectarea drepturilor omului în epoca digitală.⁹ În perioada 2000–2003 a fost ales de către utilizatorii europeni de internet în funcția de director european al ICANN, *Internet Corporation for Assigned Names and Numbers*, care este responsabilă cu politicile globale de reglementare a modului în care funcționează „numele și numerele” de pe internet.¹⁰ Este un specialist în supravegherea telecomunicațiilor și în alte tipuri de supraveghere și lucrează, în calitate de jurnalist, în domeniul industriei supravegherii cu proiectul său wiki, buggedplanet.info.¹¹ Andy lucrează în domeniul comunicațiilor criptografice și a creat împreună cu alții o companie numită Cryptophone, care vinde dispozitive pentru comunicare vocală confidențială clienților comerciali și furnizează consultanță strategică în contextul arhitecturii de rețea.¹²

JÉRÉMIE ZIMMERMANN este cofondatorul și purtătorul de cuvânt al organizației La Quadrature du Net, care militează pentru drepturile cetățeanului, cea mai proeminentă organizație europeană pentru apărarea drepturilor la anonimitate online și pentru aducerea la cunoștința publicului a atacurilor normative împotriva libertăților online.¹³ Jérémie lucrează la construirea de instrumente pe care publicul să le poată folosi pentru a participa la dezbaterile publice și pentru a încerca să schimbe lucrurile. Este implicat cel mai mult în cadrul războaielor drepturilor de autor, al dezbaterii despre neutralitatea rețelei și al altor aspecte normative care sunt esențiale pentru viitorul unui internet liber. Recent, grupul său, La Quadrature du Net, a repurtat o victorie de importanță istorică în politica europeană, orchestrând o campanie publică pentru a respinge Acordul Comercial de Combateră a Contrafacerii (ACTA) în Parlamentul European. La scurt timp după ce a participat la conversația care stă la baza acestei cărți, Jérémie a fost oprit de către doi agenți FBI în timp ce părăsea Statele Unite și a fost supus unui interogatoriu despre WikiLeaks.

Nota editorului

Pentru a crește accesibilitatea acestei cărți pentru publicul general, fiecărui participant la discuția inițială i s-a acordat posibilitatea de a dezvolta, clarifica și face adnotări la punctele principale ale argumentației sale. Ordinea generală a manuscrisului editat corespunde dinamicii discuției inițiale.

Notă despre diversele încercări de a persecuta WikiLeaks și pe cei asociați ei

În discuția care urmează se vor face mai multe referiri la evenimente recente din istoria organizației WikiLeaks și a activității sale publicistice. Acestea ar putea fi necunoscute unor cititori nefamiliarizați cu povestea WikiLeaks, așa că vor fi rezumate aici.

WikiLeaks are misiunea de a primi informații de la cei care trag semnale de alarmă, de a le face publice, iar apoi de a se apăra împotriva inevitabilelor atacuri juridice și politice. Este ceva obișnuit ca state și organizații importante să încerce să împiedice apariția publicațiilor WikiLeaks și, fiind unul dintre editorii la care se apelează când orice altceva eșuează, WikiLeaks a fost conceput să îndure astfel de dificultăți.

În 2012, WikiLeaks a scos cele mai cunoscute publicații ale sale până la această dată, dezvăluind abuzul sistematic asociat secretelor de stat în cadrul armatei și guvernului SUA. Aceste publicații sunt cunoscute sub numele de Collateral Murder, The War Logs și Cablegate.¹⁴ Reacția a fost un efort concertat și neîntrerupt al guvernului SUA și al aliaților săi de a distruge WikiLeaks.

Marele juriu pentru WikiLeaks

Ca o consecință directă a publicațiilor WikiLeaks, guvernul SUA a lansat o investigație penală în cadrul căreia mai multe organizații colaborează împotriva lui Julian Assange și a personalului WikiLeaks, precum și a susținătorilor și a presupușilor asociați ai ei. Un Mare Juriu a fost convocat în Alexandra, Virginia, cu susținerea Departamentului de Justiție și a FBI-ului, pentru a examina posibilitatea de a aduce capete de acuzare, inclusiv acuzații de conspirație conform Legii Spionajului din 1917, împotriva lui Julian Assange și a altora. Reprezentanți oficiali ai guvernului SUA au spus că investigația este „de o natură și la o scară fără precedent”. În deliberările Marelui Juriu nu sunt prezenți judecători sau avocați ai apărării. De la întocmirea Marelui Juriu, în audieri ale comisiei Congresului s-a ivit sugestia, din partea unor membri ai Congresului SUA, ca Legea Spionajului să fie folosită ca unealtă de atac împotriva jurnaliștilor care „publică în mod conștient scurgeri de informație”, lucru care pare să indice că această practică începe să se normalizeze în sistemul juridic al SUA.¹⁵

La data publicării acestui text, investigația împotriva organizației WikiLeaks continuă.¹⁶ Mai mulți oameni au fost constrânși prin mijloace juridice să depună mărturie. Procedurile judiciare de la procesul lui Bradley Manning, soldatul acuzat de furnizare de informații către WikiLeaks, au scos la iveală un dosar FBI al investigației împotriva WikiLeaks de peste 42 100 de pagini, dintre care 8 000 se referă la Manning. Bradley Manning a fost reținut fără proces timp de peste 880 de zile. Raportorul special pentru tortură al ONU, Juan Mendez, a descoperit în mod oficial că Bradley Manning a fost tratat într-o manieră crudă și inumană, și care ar putea fi considerată tortură.¹⁷

Cereri de asasinare a lui Julian Assange și grupuri operative WikiLeaks declarate public

Investigația Marelui Juriu nu este singura strategie de atac împotriva organizației WikiLeaks. În luna decembrie a anului 2010, în ajunul publicării dosarului Cablegate, mai mulți politicieni activi ai guvernului SUA au cerut asasinarea extrajudiciară a lui Julian Assange, inclusiv printr-un atac cu dronă. Senatori ai SUA au etichetat WikiLeaks drept o „organizație teroristă” și l-au numit pe Assange un „terorist high-tech” și un „combatant inamic” într-un „război cibernetic”.¹⁸

O echipă formată din 120 de angajați ai Pentagonului, numită Grupul Operativ WikiLeaks sau WTF [*WikiLeaks Task Force*], a fost alcătuită înainte de publicarea dosarelor War Logs și Cablegate și dedicată „luării de măsuri” împotriva WikiLeaks. Alte grupuri operative similare, declarate public, ale FBI, CIA și Departamentului de Stat al SUA sunt încă active.¹⁹

Cenzură directă

Într-un proces de cenzură fără precedent a unei publicații jurnalistice, guvernul SUA a exercitat presiuni asupra furnizorilor de servicii de internet să sisteze serviciile către WikiLeaks.org. În data de 1 decembrie 2010, Amazon a scos site-ul WikiLeaks de pe serverele sale de stocare, iar în data de 2 decembrie, serviciul DNS care conducea către domeniul WikiLeaks.org a fost întrerupt. Site-ul WikiLeaks a fost menținut online în timpul acestei perioade ca urmare a unui proces de „mass-mirroring”, prin care mii de susținători ai WikiLeaks au copiat site-ul și au găzduit propria lor versiune, distribuind adresele IP prin intermediul rețelilor de socializare.²⁰

Administrația Obama a avertizat funcționarii statului federal că materialele publicate de WikiLeaks rămân clasificate – chiar dacă au fost publicate de unele dintre organizațiile jurnalistice de top, inclusiv *New York Times* și *Guardian*. Funcționarilor li s-a spus că accesarea acestui material, fie de pe WikiLeaks.org sau din *New York Times*, ar fi o violare a siguranței de stat.²¹ Unele agenții ale guvernului, cum ar fi Biblioteca Congresului, Departamentul Comerțului și armata SUA, au blocat accesul la materialele WikiLeaks de pe rețelele lor. Interdicția nu a fost limitată la sectorul public. Unii angajați ai guvernului SUA au avertizat instituțiile academice că studenții care doresc să urmeze o carieră în serviciul public ar face bine să stea departe, în cercetările lor sau în activitatea online, de materialele publicate de WikiLeaks.

Cenzura financiară: blocada bancară

WikiLeaks este finanțată prin donații din partea susținătorilor ei. În luna decembrie a anului 2010, mai multe instituții bancare de importanță mondială, printre care VISA, MasterCard, PayPal și Bank of America au cedat presiunilor neoficiale ale SUA și au început să refuze serviciile financiare destinate organizației WikiLeaks. Au blocat transferurile bancare și toate donațiile făcute cu principalele carduri de credit. Deși acestea sunt instituții americane, ubicuitatea lor în economia mondială a însemnat că persoanelor care doreau să doneze, atât din America, cât și din întreaga lume, le era interzisă opțiunea de a trimite bani către WikiLeaks pentru a-i susține activitatea de publicare.

„Blocada bancară“, după cum a ajuns să fie cunoscută, este impusă în afara unor proceduri juridice sau administrative și rămâne în vigoare la data publicării celor de față. WikiLeaks a intentat procese majore în jurisdicții diferite din toată lumea

pentru a opri blocada și a repurtat o serie de victorii preliminare, iar procesele juridice continuă. Între timp, organizația WikiLeaks nu are sursă de venit, are costuri mari și operează de doi ani pe fonduri de rezervă [la data editării – 2012].

Blocada bancară este o afirmare a puterii de a controla tranzacțiile financiare între părți. Ea subminează în mod direct libertatea economică individuală. În afară de aceasta, amenințarea existențială pe care o reprezintă pentru WikiLeaks exemplifică o nouă și înspăimântătoare formă de cenzură economică mondială.²²

Câțiva presupuși asociați ai WikiLeaks împreună cu susținători și însăși echipa WikiLeaks au avut o serie de probleme misterioase cu conturile bancare – de la detaliile contului până la închiderea completă a conturilor.

Hărțuirea lui Jacob Appelbaum și a lui Jérémie Zimmermann

În data de 17 iulie 2010, Julian Assange a fost invitat să țină un discurs la conferința HOPE a hackerilor din New York. Și-a anulat discursul, iar în locul său a vorbit Jacob Appelbaum. După acest eveniment, mai multe agenții ale guvernului au condus o campanie de hărțuire împotriva lui Appelbaum și a persoanelor apropiate lui. Appelbaum a fost de nenumărate ori reținut, percheziționat, i s-a refuzat accesul la o reprezentare juridică și a fost interogat la punctele vamale de fiecare dată când a intrat sau a ieșit din Statele Unite. I s-a confiscat echipamentul și i s-au violat drepturile, fiind în același timp amenințat cu violări ulterioare ale drepturilor sale. Zeci de agenții ale SUA au fost implicate în reținerea și hărțuirea sa, de la Departamentul de Securitate Internă, Serviciul pentru Controlul Imigrației și Normelor Vamale, până la armata SUA. Aceste rețineri includ chiar și refuzul accesului

la toaletă ca metodă de forțare a colaborării. Cu toate acestea, Appelbaum nu a fost niciodată acuzat în mod formal, iar reprezentanții guvernului nu i-au spus niciodată din ce cauză este hărțuit.²³

La mijlocul lui iunie 2011, în timp ce se pregătea pentru îmbarcare la aeroportul Dulles din Washington, Jérémie Zimmermann a fost oprit de două persoane care s-au legitimat ca agenți FBI. Cei doi l-au interogat despre WikiLeaks și l-au amenințat cu arestarea și închisoarea.

Appelbaum și Zimmermann se află pe o listă lungă de prieteni, susținători sau presupuși asociați ai lui Julian Assange care au fost supuși hărțuirii și supravegherii de către agenții ale SUA, o listă care include avocați și jurnaliști aflați în exercițiul profesiei lor.

Confiscarea fără mandat a arhivelor electronice și „Cazul somației Twitter”

În data de 14 decembrie 2010, Twitter a primit o „somație administrativă” de la Departamentul de Justiție al SUA prin care i se ordona să predea informații care ar putea fi relevante pentru o investigație împotriva WikiLeaks. Somația ținea de așa-numitul „ordin 2703(d)”, care se referea la o secțiune a Legii Comunicațiilor Stocate. Conform acestei legi, guvernul SUA își atribuie autoritatea de a forța predarea arhivelor de comunicație electronică privată fără necesitatea ca un judecător să emită un mandat de percheziție – reușind efectiv să ocolească protecțiile Celui de-al Patrulea Amendament împotriva percheziției și confiscării arbitrare.

Somația cerea predarea numelor de utilizator, arhivelor de corespondență, adreselor, numerelor de telefon, detaliilor conturilor bancare și a numerelor cardurilor de credit ale persoanelor

presupuse că ar fi asociate cu WikiLeaks, inclusiv ale lui Jacob Appelbaum, ale parlamentarei islandeze Brigitta Jonsdottir, ale omului de afaceri și pionier al internetului Rop Gonggrijp și ale înseși organizației WikiLeaks. Conform termenilor somației, Twitter avea interdicția de a le spune acestor persoane de însăși existența ordinului. Cu toate acestea, Twitter a făcut cu succes apel în instanță împotriva acestei clauze de păstrare forțată a tăcerii și a câștigat dreptul să informeze persoanele vizate că le erau cerute arhivele.

După ce au fost anunțați de către Twitter cu privire la somație, în data de 26 ianuarie 2011, Appelbaum, Jonsdottir și Gonggrijp, reprezentați în instanță de către Kecker și Van Nest, Uniunea Americană a Libertăților Civile și Electronic Frontier Foundation, au cerut avocaților lor să depună împreună un dosar pentru a anula ordinul. Acesta a devenit cunoscut sub numele de „Cazul Somației Twitter”.²⁴ O altă moțiune a fost depusă de avocatul lui Appelbaum, care solicita desigilarea arhivelor încă secrete ale curții privind încercările guvernului de a strânge datele sale personale de pe Twitter și pe cele deținute de alte companii. Ambele moțiuni au fost respinse de către un judecător federal al SUA în data de 11 martie 2011. Reclamanții au făcut apel.

În data de 9 octombrie 2011, *Wall Street Journal* a dezvăluit faptul că și furnizorul de servicii de e-mail californian Sonic.net primise o somație care cerea datele lui Jacob Appelbaum. Sonic a atacat în instanță ordinul guvernului și a pierdut, dar a primit permisiunea să dezvăluie faptul că a fost forțat să predea informațiile despre Appelbaum. *Wall Street Journal* a declarat de asemenea că și Google a primit o somație similară, dar nu a specificat dacă Google a contestat decizia în instanță sau nu.²⁵

În data de 10 noiembrie 2011, un judecător federal a hotărât împotriva lui Appelbaum, Jonsdottir și Gonggrijp, decretând că Twitter trebuie să predea datele lor Departamentului de Justiție.²⁶

Reclamanții au făcut apel din nou în data de 20 ianuarie 2012, încercând să conteste refuzul de a desigila ordinele care ar fi putut fi trimise și altor companii în afară de Twitter.²⁷ În momentul publicării celor de față, procesul continuă.

Intensificarea comunicării *versus* intensificarea supravegherii

JULIAN: Dacă e să ne uităm înapoi în timp, la începutul anilor '90, în momentul amplificării mișcării cypherpunk ca răspuns la interzicerea criptografiei de către stat, mulți oameni așteptau de la internet să furnizeze comunicare liberă, necenzurată, spre deosebire de celelalte mijloace de comunicare în masă. Dar activiștii cypherpunk observaseră că, de fapt, alături de această putere, internetul mai avea și puterea de a supraveghea toate comunicările. Suntem acum în situația în care avem o intensificare a comunicării *versus* o intensificare a supravegherii. Intensificarea comunicării înseamnă că avem mai multă libertate față de persoanele care încearcă să controleze ideile și să creeze consimțământ, pe când intensificarea supravegherii intensificată înseamnă exact opusul.

Supravegherea este mult mai evidentă acum decât atunci când supravegherea în masă era făcută doar de americani, de britanici, de ruși și de câteva alte guverne, cum ar fi cel elvețian sau francez. Acum e făcută de toată lumea și aproape de fiecare stat, din pricina comercializării supravegherii în masă. Iar acum este totală, pentru că oamenii își mută toate ideile politice, comunicarea din familie și prietenii pe internet. Așadar, nu este vorba doar de o supraveghere intensificată a comunicării care exista deja, este vorba de faptul că există mult mai multă comunicare. Și nu

este vorba doar de o înmulțire a volumului comunicărilor, este vorba și de o înmulțire a tipurilor de comunicare. Toate aceste tipuri noi de comunicare care înainte ar fi fost private sunt acum interceptate în masă.

Există o bătălie între puterea pe care o are această informație strânsă de cei care au acces la ea, de aceste state ale informației care încep să se dezvolte în umbră, care fac schimb de informație unul cu celălalt, care-și dezvoltă conexiuni unul cu celălalt și cu sectorul privat, și numărul crescând al celor care folosesc internetul ca unealtă comună de comunicare.

Vreau să mă gândesc la felul în care ne vom prezenta ideile. Marea problemă pe care o am din cauză că sunt afundat în fenomenul supravegherii statale și înțeleg cum s-a dezvoltat industria transnațională a securității în ultimii douăzeci de ani este că sunt mult prea familiarizat cu aceste lucruri și din această cauză nu înțeleg cum să le văd dintr-o perspectivă a omului obișnuit. Dar acum lumea noastră este lumea tuturor, pentru că toată lumea și-a aruncat pe internet nucleul intern al vieții sale. Trebuie să comunicăm cumva lucrurile pe care le știm cât încă putem.

ANDY: Eu sugerez să nu ne uităm la acest lucru din punctul de vedere al cetățeanului, ci din punctul de vedere al celor aflați la putere. Acum câteva zile mă aflu la o conferință ciudată în Washington și m-am întâlnit cu niște tipi care aveau insigna ambasadei Germaniei. I-am abordat și le-am spus: „A, sunteți de la ambasada Germaniei“, iar ei au spus: „Nu chiar de la ambasadă, suntem de lângă München“. Am aflat până la urmă că erau dintr-o agenție de spionaj și i-am întrebat la bufetul din seara aceea: „Așadar, care este obiectivul păstrării caracterului secret?“ Mi-au spus „Păi, este acela de a încetini procesele pentru a le putea controla mai bine“. Acesta este nucleului tipului acestuia de strângere de informații, faptul de a încetini un proces luându-le oamenilor

capacitatea de a-l înțelege. A declara secret un lucru înseamnă a limita numărul oamenilor care au cunoștințele și deci capacitatea de a influența procesul.

Dacă e să ne uităm la internet din perspectiva oamenilor aflați la putere, atunci ultimii douăzeci de ani au fost înspăimântători. Ei văd internetul ca pe o boală care le afectează capacitatea de a defini realitatea, de a defini ceea ce se întâmplă, lucruri care mai apoi sunt folosite pentru a defini ceea ce știu oamenii despre ceea ce se întâmplă și capacitatea lor de a interacționa cu realitatea. Dacă ne uităm, să zicem, la Arabia Saudită, unde, în urma unor împrejurări istorice, liderii religioși și cei care dețin majoritatea țării reprezintă același grup, interesul față de schimbare este zero. Poate între zero și minus cinci, mai degrabă. Percep internetul ca pe o boală și își întreabă consilierii: „Aveți vreun medicament împotriva lucrului ăstuia? Trebuie să ne imunizăm în caz că ne va afecta țara, în caz că lucrul ăsta numit internet vine peste noi”. Iar răspunsul este supravegherea în masă. Răspunsul este: „Trebuie să-l controlăm în întregime, trebuie să filtrăm, trebuie să știm tot ce fac”. Iar asta este ceea ce s-a întâmplat în ultimii douăzeci de ani. A existat o investiție masivă în supraveghere pentru că cei aflați la putere s-au temut că internetul le va afecta tipul de guvernare.

JULIAN: Și totuși, în ciuda acestei supravegheri masive, comunicarea în masă a dus la faptul că milioane de oameni au reușit să ajungă la un consens în mod rapid. Dacă poți trece foarte repede de la o poziție normală la una nouă, de consens general, atunci, deși statul ar putea să vadă ce se întâmplă, nu are destul timp pentru a elabora un răspuns eficient.

Acestea fiind spuse, a existat un protest organizat pe Facebook în 2008, în Cairo. Guvernul Mubarak a fost luat prin surprindere de acest lucru, iar din această cauză acei oameni au fost depistați cu ajutorul Facebook-ului.²⁸ În 2011, într-un manual care

a fost unul dintre cele mai importante documente folosite în revoluția egipteană, pe prima pagină scria: „Nu folosiți Twitter sau Facebook“ pentru a distribui manualul, iar pe ultima pagină scria „Nu folosiți Twitter sau Facebook“ pentru a distribui manualul.²⁹ Cu toate acestea, foarte mulți cetățeni egipteni au folosit Twitter și Facebook. Dar motivul pentru care au supraviețuit a fost acela că revoluția a avut succes. Dacă nu ar fi avut succes, acei oameni s-ar fi aflat într-o poziție foarte, foarte neplăcută. Și să nu uităm că președintele Murabak a tăiat internetul în Egipt destul de devreme. Se poate dezbate dacă oprirea internetului a facilitat sau a încetinit revoluția. Unii cred că a facilitat-o, din cauză că oamenii au trebuit să iasă în stradă pentru a afla ce se petrecea și, odată ce ai ieșit în stradă, ești în stradă. Iar oamenii au fost afectați în mod direct pentru că nu le mai funcționau telefoanele mobile și internetul.

Prin urmare, ca să aibă succes, e nevoie de o masă critică, trebuie să se întâmple rapid și trebuie să învingă, pentru că dacă nu învinge, aceeași infrastructură care a permis ca un consens rapid să se dezvolte va fi folosită pentru a-i depista și marginaliza pe toți acei oameni care au fost implicați în crearea consensului.

Deci acesta a fost cazul Egiptului, care, da, era un aliat al SUA, dar care nu face parte din alianța serviciilor de spionaj vorbitoare de limba engleză formată din SUA, Regatul Unit, Australia, Noua Zeelandă și Canada. Acum hai să ne imaginăm revoluția egipteană pornind în Statele Unite – ce s-ar întâmpla cu Facebook și Twitter? Ar fi preluate de stat. Iar dacă revoluția nu ar avea succes, ar fi investigate, după cum sunt și acum, de către CIA și FBI, pentru a găsi detalii despre cei care au fost participanții-cheie.

JÉRÉMIE: Este dificil să disociem supravegherea de control. Trebuie să ne ocupăm de ambele. Asta mă interesează pe mine

mai mult – controlul internetului, fie că vine din partea guvernului, fie că vine din partea corporațiilor.

JACOB: Cred că este clar că cenzura este un produs secundar al supravegherii în general, fie că este vorba de autocenzură, fie că e vorba de cenzură tehnică efectivă, și cred că un aspect important legat de modul în care comunicăm lucrul acesta omului de rând este să o facem nontehnic. De exemplu, dacă am construi drumuri în același fel în care construim internetul, fiecare drum ar avea camere de supraveghere și microfoane la care nu ar avea acces nimeni în afară de poliție sau de cineva care s-ar preface că face parte din poliție.

JULIAN: La asta se ajunge, Jake, în Regatul Unit.

JACOB: Când construiești un drum nu e necesar ca fiecare centimetru să fie monitorizat cu o supraveghere perfectă care să fie accesibilă doar unui grup secret de oameni. Explicându-le oamenilor de rând că acesta este felul în care construim drumurile pe internet și apoi cerându-le să folosească acele drumuri – acesta este un lucru cu care oamenii obișnuiți pot rezona, atunci când realizează că constructorii inițiali ai drumului nu vor fi tot timpul și cei care-l controlează.

ANDY: Dar unii oameni nici nu construiesc drumuri. Construiesc o grădină și invită pe toată lumea să stea dezbrăcată. Și iată-ne ajunși la Facebook! Este o pledoarie pentru a-i face pe oameni să se simtă confortabil cu dezvăluirea datelor personale.

JACOB: Exact. Oamenii au primit compensații pentru că au fost în Stasi – securitatea de stat a fostei Germanii de Est – și primesc compensații și pentru că fac parte din Facebook. Doar că pe Facebook sunt compensați cu credite sociale – și-o pun cu vecinul – în loc să fie plătiți în mod direct. Și este important să ne

referim la aspectul uman, pentru că nu este vorba despre tehnologie, este vorba despre controlul prin supraveghere. În anumite aspecte este panopticumul perfect.³⁰

JULIAN: Mă interesează foarte mult filosofia tehnicii. Tehnica nu înseamnă doar o tehnologie, ci înseamnă, să spunem, consensul majorității într-un consiliu, sau structura unui parlament – este interacțiunea sistematizată. De exemplu, am impresia că sistemele feudale s-au născut din tehnologia morilor. Odată ce ai mori centralizate, pentru care e nevoie de investiții uriașe și care pot fi controlate fizic foarte ușor, e firesc să apară relații feudale. Cu trecerea timpului se pare că am elaborat tehnici din ce în ce mai sofisticate. Unele dintre aceste tehnici pot fi democratizate, pot fi răspândite tuturor. Dar majoritatea – datorită complexității lor – sunt tehnici care se formează în urma unor organizații foarte interconectate, cum ar fi corporația Intel. Poate că tendința fundamentală a tehnicii este să treacă prin aceste perioade de descoperire a tehnicii, centralizare a tehnicii, democratizare a tehnicii – când cunoașterea modului ei de funcționare se răspândește în rândul următoarei generații educate. Dar cred că tendința generală a tehnicii este să centralizeze controlul în mâinile acelor oameni care controlează resursele fizice ale tehnicilor.

Exemplul suprem al acestui lucru este, cred, ceva de genul unui producător de semiconductoare, unde ai nevoie de o asemenea ordine încât chiar și aerul trebuie să fie pur, unde ai nevoie de o fabrică în care luzionează mii de oameni care trebuie să poarte plase de păr pentru a ține orice particulă de piele uscată, orice fir de păr departe de procesul de producție a semiconductoarelor, acesta fiind un proces extrem de complicat, format din mai mulți pași. Iar organizația producătoare de semiconductoare este în posesia unei cunoașteri rezultate în urma a milioane de ore de cercetări. Dacă acele lucruri sunt populare, și sunt, și dacă se află la baza

internetului, atunci codificată în eliberarea internetului se află și producția de semiconductoare. Și codificată în producția de semiconductoare se află și capacitatea oricui are controlul fizic asupra producătorului de semiconductoare să extragă concesiile uriașe.

Așadar, la baza revoluției comunicării high-tech – și a libertății pe care am extras-o din aceasta – se află întreaga economie de piață modernă, neoliberală, transnațională și globalizată. De fapt, ea reprezintă vârful ei. Este maximumul, în termeni de realizări tehnologice, a ceea ce economia neoliberală modernă globalizată poate produce. Internetul se sprijină pe relații comerciale extrem de complexe între producătorii de fibră optică, producătorii de semiconductoare, companiile miniere care extrag toate aceste lucruri și toți lubrifianții financiari care înlesnesc schimbul, tribunalele care impun legile proprietății private și așa mai departe. Deci este chiar vârful piramidei întregului sistem neoliberal.

ANDY: Referitor la ce spuneai despre tehnică, când Johannes Gutenberg a inventat presa de tipar, ea a fost chiar interzisă ocazional în unele regiuni ale Germaniei și de aceea s-a răspândit în toată țara, fiindcă atunci când era interzisă într-o regiune, afacerea se muta într-o altă jurisdicție.³¹ Nu am studiat chestiunea în toate detaliile, dar ceea ce știu este că Biserica Romano-Catolică a fost deranjată fiindcă se elimina monopolul deținut de ea pe tipărirea cărților, așa că de îndată ce aveau probleme de ordin juridic, se mutau undeva unde presa nu era interzisă. Într-un fel, acest lucru a ajutat la răspândirea ei.

Internetul a fost puțin diferit, cred, din cauză că pe de-o parte ai mașini care pot fi folosite ca unități de producție, așa cum a fost, într-un fel, cazul chiar și cu Commodore 64, deși majoritatea l-au folosit în alte scopuri.

JULIAN: Deci pe orice mic dispozitiv pe care îl aveai îți puteai instala propriul software.

ANDY: Da. Și îl puteai folosi și pentru a răspândi idei. Dar pe de altă parte, din punct de vedere filosofic, după cum a spus și John Gilmore – unul dintre fondatorii filialei americane a Electronic Frontier Foundation – la începutul anilor '90, când internetul atinsese întinderea globală: „Rețeaua consideră cenzura ca fiind dăunătoare și o ocolește”.³² După cum știm astăzi, această afirmație a fost un amestec de interpretare tehnică și de viziune optimistă de impact, un fel de năzuință nerealistă și profeție autoîmplinită.

JULIAN: Dar a fost adevărat pentru Usenet, care este un sistem de e-mail de grup, dacă vreți, care a apărut acum treizeci de ani. Pentru a explica Usenet într-o manieră simplă, imaginați-vă că nu există nici o diferență între oameni și servere și că fiecare persoană are propriul său server Usenet. Se scrie ceva și se trimite către unul sau doi oameni. Aceștia (în mod automat) verifică dacă au deja mesajul. Dacă nu-l au deja, îl preiau și-l trimit tuturor celor cu care sunt conectați. Și așa mai departe. În consecință, mesajul ajunge la toată lumea și toată lumea primește, într-un final, o copie. Dacă una dintre persoane cenzurează, ea este pur și simplu ignorată, nu schimbă cu nimic situația. Mesajul continuă să se răspândească prin intermediul tuturor persoanelor care nu cenzurează. Gilmore vorbea despre Usenet, nu vorbea despre internet. Și nu vorbea nici despre pagini web.

ANDY: Deși ceea ce spui este corect, interpretarea cuvintelor sale și impactul lor pe termen lung au fost de natură să producă oameni care se percep pe ei înșiși ca fiind internetul. Oamenii spuneau: „Ok, există cenzură, o vom ocoli”, în timp ce politicianul fără pricepere tehnică se gândea: „Ce rahat, există o nouă tehnologie care ne limitează controlul asupra sferei de informații”. Deci cred că Gilmore, care a fost unul dintre premergătorii mișcării cypherpunk, a făcut un lucru foarte bun ducând lucrurile în

această direcție care a inspirat întreaga manieră cripto-anarhistă de a avea propria formă de comunicare anonimă fără a te teme că vei fi urmărit.

JÉRÉMIE: Eu văd o diferență în cazul a ceea ce descriem noi ca fiind răspândirea tehnologiei, pentru că în cazul morii sau al presei de tipar trebuia doar să privești una din cele două pentru a înțelege cum funcționează, pe când acum proiectăm controlul din ce în ce mai mult în interiorul tehnologiei. Controlul este încorporat în tehnologie. Dacă ar fi să te uiți la un computer modern, în cele mai multe cazuri nici nu ai fi în stare să-l deschizi și să înveți toate componentele. Și toate componentele se află în cutiuțe mici – nu poți să știi ce face fiecare.

ANDY: Din cauza complexității?

JÉRÉMIE: Din cauza complexității, dar și din cauză că tehnologia ca atare nu este făcută pentru a fi înțeleasă. Așa stau lucrurile în cazul tehnologiei proprietare.³³ Cory Doctorow o descrie în „The War on General-Purpose Computing”.³⁴ Acolo unde computerul este un dispozitiv generalist, poți face totul cu el. Poți procesa orice informație ca input; o poți transforma în orice ca output. Și construim din ce în ce mai multe aparate care sunt astfel de computere cu scop generalist, dar a căror utilizare e restricționată doar la a fi GPS-uri sau telefoane sau playere MP3. Construim din ce în ce mai multe dispozitive în care controlul este deja încorporat, pentru a-i interzice utilizatorului să facă anumite lucruri.

JULIAN: Controlul este integrat în dispozitiv pentru a împiedica oamenii să înțeleagă dispozitivul și să-l modifice, dându-i alt scop decât cel pentru care l-a proiectat producătorul, dar ceea ce se întâmplă acum este și mai rău, pentru că dispozitivul este conectat la rețea.

JÉRÉMIE: Da, astfel încât să poată conține funcția de monitorizare a utilizatorului și a datelor sale. De aceea software-ul liber este atât de important pentru o societate liberă.

ANDY: Sunt complet de acord că avem nevoie de computerul cu scop generalist, dar în dimineața asta, când încercam să vin aici de la Berlin, avionul și-a întrerupt decolarea – este prima oară când mi s-a întâmplat lucrul acesta. Avionul a tras pe dreapta, iar căpitanul ne-a spus: „Doamnelor și domnilor, am avut o defecțiune la sistemele electronice, așa că am decis să ne oprim și să repornim sistemele“. Și chiar m-am gândit: „Rahat, parcă ar fi restartarea la Windows, Control Alt Delete – poate funcționează!“ Așa că nu aș fi foarte nemulțumit dacă am avea un computer cu scop unic pe avion care să facă doar asta și să o facă foarte bine. Dacă stau într-o mașinărie zburătoare nu vreau ca piloții să fie distrași jucându-se Tetris sau ca avionul să fie infectat cu Stuxnet sau mai știu eu ce.³⁵

JÉRÉMIE: Avionul ca atare nu-ți procesează datele personale, nu are nici un control asupra vieții tale.

ANDY: Păi o mașină zburătoare are control asupra vieții mele pentru o vreme.

JACOB: Cred că putem descrie cel mai bine argumentul lui Cory spunând că nu mai există mașini, nu mai există avioane, nu mai există aparate auditive; există computere cu patru roți, computere cu aripi și computere care te ajută să auzi. Și o chestiune importantă nu este aceea dacă sunt sau nu computere cu scop unic, ci dacă putem verifica sau nu că fac lucrul pe care spun că îl fac, și dacă înțelegem sau nu cât de bine îl fac. Deseori unele persoane încearcă să susțină că au dreptul să țină aceste lucruri sub cheie, păstrându-le secrete, și fie proiectează calculatoare complexe,

fie ne pun piedici de ordin juridic în calea înțelegerii lor. Acest lucru este periculos pentru societate, fiindcă știm că oamenii nu acționează tot timpul în interesul nostru comun, după cum știm și că oamenii greșesc – nu din răutate –, astfel că ținerea acestor lucruri sub cheie este foarte periculoasă din mai multe puncte de vedere, unul dintre acestea fiind faptul că suntem imperfecti. Aceasta este realitatea. Faptul de a avea acces la schemele sistemelor care ne guvernează viața este unul din motivele pentru care software-ul liber este important, dar este de asemenea motivul pentru care hardware-ul liber este important. Ne îmbunătățește capacitatea de a face liber investiții sustenabile, de a îmbunătăți sistemele pe care le folosim și de a afla dacă sistemele acestea funcționează cum ar trebui. Dar dincolo de libertate, acesta este și motivul pentru care e important să înțelegem aceste sisteme, pentru că atunci când nu le înțelegem, există o tendință generală de a ceda în fața autorității, în fața oamenilor care le înțeleg și care pot să le controleze, chiar dacă aceștia nu înțeleg esența lucrului ca atare. De aceea se vorbește atât despre războiul cibernet – din cauză că unii oameni care par să aibă autoritatea în ceea ce privește războiul încep să vorbească despre tehnologie ca și cum ar înțelege-o. Astfel de oameni vorbesc deseori despre războiul cibernet și nici unul dintre ei, nici măcar unul, nu vorbește despre menținerea păcii prin mijloace cibernetice sau de orice ar ține de menținerea păcii. Vorbesc tot timpul despre război din cauză că asta e treaba lor și încearcă să controleze procesele tehnologice și juridice pentru a-și promova interesele proprii. Așadar, când nu deținem controlul asupra tehnologiei noastre, astfel de persoane vor dori să o folosească pentru scopurile lor, în speță pentru război. Iar asta e rețeta pentru niște lucruri destul de înspăimântătoare – așa cred că s-a ajuns la Stuxnet –, iar unele persoane altminteri rezonabile vor sugera, în timp ce SUA se află în război, că astfel de tactici ar putea cumva să prevină războiul.

Acest argument este, poate, unul rezonabil pentru o țară care nu invadează în mod activ alte națiuni, dar cu greu poate fi unul credibil în contextul unei națiuni implicate în invadări multiple și concomitente.

Militarizarea spațiului cibernetic

JULIAN: Am observat că ne aflăm acum într-un proces de militarizare a spațiului cibernetic, în sensul unei ocupații militare. De fiecare dată când comunicăm pe internet, când comunicăm folosind telefoanele mobile, care acum sunt legate la internet, comunicările noastre sunt interceptate de organizații militare de spionaj. Este ca și cum ai avea un tanc în dormitor. Între tine și soție se află un soldat atunci când vă trimiteți SMS-uri. În ceea ce privește comunicările noastre, trăim cu toții sub legea marțială, doar că nu putem vedea tancurile – dar ele sunt aici. În acest sens, internetul, care ar fi trebuit să fie un spațiu civil, a devenit un spațiu militarizat. Dar internetul este spațiul nostru, pentru că îl folosim cu toții pentru a comunica unii cu ceilalți și cu membrii familiei noastre. Comunicările cele mai intime din viețile noastre private se fac acum pe internet. Deci, de fapt, viețile noastre private au intrat într-un spațiu militarizat. Este ca și cum ai avea un soldat sub pat. Aceasta este militarizarea vieții civile.

JACOB: Chiar înainte să vin aici mi s-a propus să fiu antrenor al echipei Laboratorului de Cercetare în domeniul Securității și Confidențialității al Universității din Washington pentru concursul Pacific Rim Collegiate Cyber Defense. În ultimul moment

mi s-a propus să fiu consilier. Am petrecut o groază de timp concurând într-o competiție de război cibernetic în care SPAWAR, o ramură civilă a marinei SUA, ce include și servicii constând în teste de penetrare și care face atât hacking ofensiv, cât și hacking defensiv, era ceea ce se numește de obicei Echipa Roșie.³⁶ Ceea ce fac ei este să-i atace pe toți cei care joacă, iar sarcina fiecărei echipe este să-și apere sistemele informatice pe care le-au primit la începutul competiției, fără să știe dinainte ce se va întâmpla. Nu știi ce fel de sisteme vei apăra și nici măcar nu este clar cum funcționează punctajul la început, așa că încerci să dai tot ce ai mai bun și să speri.

JULIAN: Ești sigur că ăsta e un joc? Poate nu e un joc!

JACOB: Nu, primești doar niște calculatoare pe care trebuie să le aperi, și alții încearcă să le spargă și să preia controlul-sistemelor. Este ca un joc de-a Prinde Steagul la o conferință de hackeri sau ceva de genul, și e interesant pentru că băieții ăștia au multe instrumente, au scris software.³⁷

JULIAN: Dar care e scopul jocului ăstuia – din perspectiva marinei SUA?

JACOB: Păi, în cazul lor, sponsorizează asta pentru că vor să formeze astăzi războinicii ciberneticici de mâine și, de exemplu, ți-am adus un carnețel de la CIA, pentru că recrutau. Era un tip acolo care se numea Charlie – Charlie de la CIA –, care explica că dacă vrei să vii să te angajezi la CIA, aceasta este o ocazie foarte bună pentru a lucra în lumea reală. Și erau acolo și oamenii de la SPAWAR, și era și Microsoft care recruta. Ideea era să antrenezi toți acei oameni, toate acele echipe, să ajungă la Campionatul Național și să câștige și să „apere țara“, iar apoi să poată ajunge să facă hacking ofensiv ca războinicii ciberneticici, nu doar ca

apărători cibernetici. Am avut un punctaj de 4 000 de puncte, care a fost punctajul cumulat al echipelor de pe locurile doi, trei și patru. A fost de fapt chiar mai mare decât toate punctele lor puse împreună.

JULIAN: Da, da, da.

JACOB: Nu a fost mulțumită mie – discursul meu de motivare a fost un fel de „Băieți, cel mai mare întuneric este întotdeauna fix înainte să se facă beznă” – și nici nu sunt prea bun la antrenat – băieții ăștia sunt foarte buni. Dar a fost interesant pentru că modul în care era prezentată toată chestia era în termeni de război, așa că ziceau: „Hei, vrem să vă auzim strigătul de război”. Îți venea să zici: „Poftim? Cum adică?” Asta spuneau în timpul prânzului, de exemplu, când luau o pauză de la apărarea sistemelor noastre. Formulau totul în termeni de atacare a sistemelor și de război cibernetic și de măreție a acestui fel de a gândi. Și, foarte interesant, în afară de echipa cu care lucram eu, am avut impresia că mulți dintre acei oameni aveau mari bătaii de cap, pentru că nu erau instruiți să folosească Arta Războiului – era mai degrabă ca la Cupa Sysadmin, oameni care apără sisteme – și mi s-a părut dezgustător.³⁸ M-am simțit foarte bizar, pentru că toți oamenii ăștia care aveau experiența războiului veneau cu o perspectivă de război, dar nu predau strategie, erau foarte concentrați pe retorica apărării acestor sisteme sau a atacului acestor sisteme și aveau atâta război în cap încât chiar încercau să incite pe toată lumea într-un soi de fervoare patriotică. Nu promovau gândirea creativă sau vreun fel de cadru pentru analiză independentă; îndemnau la o mentalitate-a-angrenajului-într-o-mașinărie, a cuiva care urmează ordinele pentru binele națiunii. Nu mai avusesem o asemenea experiență până atunci. Mi s-a făcut rău și majorității celor din echipa mea le-a fost greu s-o digere sau măcar s-o ia în serios.

JULIAN: Crezi că e un antrenament standard al marinei SUA și că încearcă acum să-l folosească într-un alt domeniu? Este oare o decizie venită din partea conducerii SUA pe domeniul cibernetic – o decizie strategică internațională?

ANDY: Mai degrabă ca în cazul naziștilor care aveau acele tabere în care erau antrenați copii.

JACOB: *Sie können das sagen weil du bist Deutsche.* Poți să spui asta pentru că ești neamț. Nu, nu e așa. Marina SUA se implică doar din cauză că guvernul SUA sponsorizează toată chestia asta. Mi-au propus să-i pregătesc pentru că aveau nevoie de cineva care să-i pregătească și am acceptat pentru că-mi plăceau băieții implicați, studenții. Dar, de fapt, lucrul se rezumă la faptul că guvernul SUA încearcă să împingă oamenii în chestia asta și încearcă să o facă dintr-o perspectivă a naționalismului. Este o competiție foarte stranie pentru că, pe de-o parte, este bine să știi cum să-ți aperi sistemul și e bine să înțelegi infrastructura pe care se bazează viețile noastre; dar, pe de altă parte, nu încercau să convingă oamenii să le înțeleagă, încercau să le inducă un soi de fervoare pentru a-i face să le placă genul ăsta de activitate.

ANDY: Din păcate, interesul Statelor Unite în ceea ce privește menținerea securității sistemelor este total limitat, pentru că își doresc ca sistemele să fie vulnerabile, ca ei să poată prelua controlul asupra lor. Încercarea de a controla criptografia mondială nu a mers atât de departe precum și-au dorit la început Statele Unite, undeva prin 1998, când David Aarons, subsecretarul SUA însărcinat cu comerțul internațional, a fost într-un turneu mondial pledând pentru necesitatea accesului guvernului la parolele tuturor.³⁹ Dar criptografia este încă considerată o tehnologie cu o așa-numită dublă întrebuințare, iar exportul său în alte țări, sub forma produselor pentru utilizatorul final, este limitat prin lege

stabilită în cadrul unei convenții mondiale numite Acordul de la Wassenaar.⁴⁰ E un lucru care ar putea suna rezonabil, în contextul declarării anumitor națiuni și a acțiunilor lor ca fiind „ticăloase“, dar el indică dimensiunea standardului dublu, căci, deocamdată, tehnologia de supraveghere a telecomunicațiilor nu este reglementată prin controlul exporturilor.⁴¹

JULIAN: Andy, tu ai conceput ani de zile telefoane criptografice. Despre ce fel de supraveghere în masă se poate vorbi referitor la telecomunicații? Spune-mi care este vârful tehnologic în ceea ce privește industria spionajului/supravegherii en-gros făcute de guvern?

ANDY: Stocarea în masă – care presupune stocarea tuturor telecomunicațiilor, a tuturor apelurilor vocale, a tuturor datelor de trafic, a tuturor modurilor în care grupurile folosesc Serviciul de Mesaje Scurte (SMS), dar și a tuturor conectărilor la internet, care în unele cazuri conțin cel puțin serviciile de e-mail. Dacă compari bugetul armatei cu costul supravegherii și al războinicilor cibernetici, sistemele obișnuite de armament costă mult. Războinicii cibernetici sau supravegherea în masă sunt foarte ieftine comparate chiar și cu un singur avion. Un avion militar te costă între...

JULIAN: În jur de o sută de milioane.

ANDY: Iar stocarea devine în fiecare an din ce în ce mai ieftină. La Chaos Computer Club am făcut chiar niște calcule: poți să stochezi, la o calitate decentă, toate apelurile telefonice făcute într-un an în Germania cu circa 30 de milioane de euro, iar asta include și cheltuielile administrative, deci doar stocarea ar costa în jur de 8 milioane de euro.⁴²

JULIAN: Și există chiar companii, cum este VASTech în Africa de Sud, care scot aceste sisteme la vânzare la prețul de 10 milioane

de dolari pe an.⁴³ „Vă vom intercepta toate apelurile și vom stoca în masă toate apelurile interceptate.“ Dar în ultimii ani s-a făcut o trecere de la interceptarea tuturor comunicațiilor dintre o țară și alta și selectarea acelor oameni pe care vrei să-i spionezi și încredințarea lor în seama altor oameni, la interceptarea tuturor comunicațiilor și la stocarea lor permanentă.

ANDY: Ca să dau o explicație oarecum istorică a acestui fenomen, pe vremuri erai o țintă din cauza poziției diplomatice, din cauza companiei pentru care lucrai, din cauză că erai suspectat că ai fi făcut ceva sau erai în contact cu oameni care chiar făceau ceva, și apoi se aplicau măsurile de supraveghere împotriva ta. În ziua de azi pare mult mai eficient să spui „Luăm totul și triem mai târziu“. Deci chiar au stocare pe termen lung, iar modalitatea cea mai bună de a descrie cele două capitole ale acestei industrii sunt abordarea „tactică“ și abordarea „strategică“. Tactic înseamnă: „În acest moment, în timpul acestei întâlniri, trebuie să interceptăm totul, trebuie să infiltrăm pe cineva cu un microfon sau să avem sisteme de supraveghere prin GSM (Sistem Global pentru Comunicațiile Mobile) într-o mașină, gata instalate, capabile să intercepteze imediat tot ce se spune, fără să avem nevoie de amestecul operatorului de rețea, fără să avem nevoie să obținem un mandat de percheziție sau ceva de genul ăsta de la poliție, fără să avem nevoie de proceduri juridice – s-o facem pur și simplu“. Abordarea strategică este să o faci automat, să înregistrezi pur și simplu totul și să sortezi după aceea înregistrările, folosind sisteme analitice.

JULIAN: Deci interceptarea strategică este să iei tot ce se transmite printr-un satelit de telecomunicații, să iei tot ce trece printr-un cablu de fibră optică.

ANDY: Pentru că nu știi niciodată când cineva este suspect.

JACOB: Există în Statele Unite ceva ce se numește cazul NSA AT&T – al doilea caz: *Hepting vs AT&T*. În orașul Folsom din California, Mark Klein, un fost tehnician al uriașei companii de telecomunicații AT&T, a scos la iveală faptul că NSA, Agenția Națională de Securitate SUA, capta toate datele pe care i le putea oferi AT&T. Pur și simplu le lua en gros – atât date, cât și apeluri telefonice –, așadar de fiecare dată când ridicam receptorul sau mă conectam la internet în San Francisco în timpul perioadei despre care a vorbit Mark Klein, știm că pe pământ american, împotriva cetățenilor SUA, NSA primea totul.⁴⁴ Sunt sigur că au folosit datele interceptate respective în investigații împotriva persoanelor din Statele Unite, lucru care ridică tot soiul de probleme constituționale interesante, deoarece rețin datele pentru totdeauna.

JÉRÉMIE: Mai este și exemplul Eagle, sistemul vândut Libiei lui Gaddafi de către compania franceză Amesys, iar pe documentul comercial scria „Mecanism de interceptare națională”. Este o cutie mare pe care o pui undeva și stai și asculți conversațiile întregului popor.⁴⁵

JULIAN: Acum zece ani, lucrurile acestea erau văzute drept ceva de domeniul fantasticului, un lucru în care credeau doar oamenii paranoici, dar costurile interceptării în masă au scăzut în așa măsură încât până și o țară ca Libia, cu resurse relativ puține, a ajuns să o facă, cu tehnologie franceză. În realitate, majoritatea țărilor au ajuns în acest punct, în ceea ce privește interceptarea. Următorul mare pas va fi eficiența cu care vor fi înțelese informațiile interceptate și stocate, și eficiența reacției față de acestea. Acum are loc, în multe țări, interceptarea strategică a întregului trafic care intră sau iese din țară, dar acțiunile care urmează acestei interceptări, cum ar fi blocarea automată a conturilor bancare, sau desfășurarea forțelor poliției, sau marginalizarea anumitor

grupuri, sau emanciparea altora, sunt lucruri până la care mai e încă un pas. Siemens vinde o platformă pentru agenții de spionaj care produce acțiuni automate. Așadar, când persoana țintă A se află la un anumit număr de metri de persoana țintă B conform interceptării telefoanelor mobile, iar persoana țintă A primește un e-mail care menționează ceva – un cuvânt-cheie – se declanșează acțiunea. E pe punctul de a se produce.

Combaterea supravegherii totale cu ajutorul legilor omului

JÉRÉMIE: Prin urmare, acum este fapt real acela că tehnologia permite supravegherea totală a tuturor comunicațiilor. Apoi mai este și cealaltă față a monedei, anume ce facem cu ceea ce interceptăm. Putem admite că pentru ceea ce numești supraveghere tactică există utilizări legitime – diverși investigatori care anchetează ticăloși sau rețele de ticăloși și așa mai departe s-ar putea să aibă nevoie, sub supravegherea unei autorități judiciare, să se folosească de astfel de instrumente –, dar întrebarea este: unde trasăm limita acestei supravegheri judiciare, unde trasăm limita controlului pe care-l pot avea cetățenii asupra folosirii acestor tehnologii? Este o problemă de politică. Și când ajungem la problemele acestea de politică, se întâmplă ca unii politicieni să fie rugați să semneze ceva fără să înțeleagă tehnologia de la bază, și cred că noi, ca cetățeni, avem un rol, nu doar să explicăm, inclusiv politicienilor, cum funcționează tehnologia, ci și să intrăm în dezbaterile politice din jurul folosirii acestor tehnologii. Știu că în Germania a existat o mișcare masivă împotriva reținerii generalizate de date, care a dus la răsturnarea Legii Reținerii Datelor în fața Curții Constituționale.⁴⁶ Există acum în Uniunea Europeană o dezbatere despre revizuirea Directivei Reținerii Datelor.⁴⁷

ANDY: Descrui aici teoria statului democratic, care, desigur, trebuie să filtreze niște ticăloși ici și colo și să le asculte telefoanele, pe baza unei hotărâri judecătorești și cu supraveghere juridică, în scopul asigurării că procedura se face cum se cuvine. Problema este că autoritățile trebuie să acționeze în concordanță cu legea. Dacă nu fac asta, atunci la ce mai sunt bune? Mai cu seamă în cazul abordării acesteia strategice, unele state democratice europene cumpără masiv aparate care le permit să acționeze tocmai în afara legii în ceea ce privește interceptarea, pentru că nu au nevoie de o hotărâre judecătorească, au nevoie doar să pornească aparatele și să o facă, iar tehnologia asta nu poate fi controlată.

JULIAN: Dar sunt oare două abordări în ceea ce privește supravegherea în masă a statului: legile fizicii și legile omului? Una este să folosești legile fizicii construind efectiv instrumente care previn interceptarea. Cealaltă este să pui în aplicare prin lege controale democratice pentru a te asigura că oamenii vor avea nevoie de mandate și așa mai departe și să încerci să câștigi puțină responsabilizare legislativă. Dar interceptarea strategică nu poate face parte din asta, nu poate fi limitată în mod semnificativ prin legislație. Interceptarea strategică se ocupă cu interceptarea *oricui*, indiferent dacă e vinovat sau nevinovat. Trebuie să ne amintim că ține de nucleul cercurilor conducătoare faptul de a efectua asemenea supraveghere. Va exista întotdeauna o lipsă de voință politică de a dezvălui acțiunile de spionaj ale statului. Iar tehnologia este în sine atât de complexă, iar folosirea sa în practică atât de secretă, încât nu poate exista o supraveghere democratică semnificativă.

ANDY: Sau îți spionezi propriul parlament.

JULIAN: Dar alea sunt scuze – mafia și spionajul străin –, sunt scuze pentru ridicarea unui astfel de sistem, astfel ca oamenii să accepte.

JACOB: Cei Patru Călăreți ai Apocalipsei Informatice: pornografia infantilă, terorismul, spălarea de bani și Lupta împotriva unor Droguri.

JULIAN: Odată ce ai instalat acest sistem de supraveghere, având în vedere că este complex, având în vedere că este conceput să funcționeze în secret, nu este oare adevărat că el nu poate fi reglementat politic? Cred că, exceptând state foarte mici ca Islanda, dacă nu există circumstanțe revoluționare nu va fi posibil să controlezi interceptarea în masă cu legislație și politici publice. Pur și simplu nu se va întâmpla lucrul acesta. Este mult prea ieftin și prea ușor să ocolești răspunderea politică și să interceptezi realmente. Suedia a avut în 2008 un proiect de lege privind interceptarea, cunoscut sub numele de FRA-lagen, care prevedea că agenția suedeză de spionaj, FRA, putea intercepta în masă, în mod legal, toate comunicațiile care treceau prin țară și le putea trimite Statelor Unite, cu unele limitări.⁴⁸ Dar cum poți să pui în aplicare acele limitări odată ce ai instalat sistemul de interceptare, iar organizația care-l folosește este o agenție secretă de spionaj? E imposibil. Iar, în realitate, unele cazuri care au ieșit la iveală au arătat că FRA încălcase legea cu mai multe prilejuri. Multe țări o fac în afara legii, fără absolut nici o acoperire legislativă. Deci suntem cumva norocoși dacă, la fel ca în exemplul suedez, s-a decis, pentru propria protecție față de urmărirea în instanță, să se intre în legalitate schimbând legea. Iar aceasta este situația celor mai multe țări – se face interceptare en gros, iar de fiecare dată când se fac propuneri legislative, se fac pentru a-i proteja pe cei care o fac.

Tehnologia aceasta este foarte complexă; de exemplu, în cazul dezbaterii din Australia și din Regatul Unit în ceea ce privește legislația propusă pentru a intercepta toate metadatele, majoritatea populației nu înțelege valoarea metadatelor și nici măcar cuvântul în sine.⁴⁹ A intercepta toate metadatele înseamnă că

trebuie să construiești un sistem care interceptează fizic toate datele, iar apoi aruncă la gunoi totul în afară de metadate. Dar nu poți avea încredere într-un astfel de sistem. Nu există nici o modalitate prin care să-ți dai seama dacă nu cumva interceptează și stochează de fapt toate datele, neavând ingineri foarte pricepuți și autorizați să meargă și să verifice exact ce se petrece, și nu există voință politică pentru a acorda accesul în acest sens. Problema se înrăutățește, din cauză că secretele și complexitatea sunt un amestec toxic. Tăinuit prin complexitate. Tăinuit prin caracterul secret. Fenomenul interceptării este incontrollabil prin însăși natura sa. Incontrollabilitatea este o caracteristică a lui. Este periculos prin însuși felul în care a fost conceput.

JÉRÉMIE: Eu nu spun că abordarea politică poate funcționa. Spun că aceasta este teoria despre cum ar trebui să funcționeze un sistem democratic și, într-adevăr, chiar și cu această teorie ai serviciile secrete, cărora le este permis să nu respecte regulile pentru forțele de poliție și investigatorii standard. Deci chiar dacă limităm cum trebuie comportamentul investigatorilor standard, ar exista alți oameni care ar putea folosi aceste tehnologii. Dar adevărata întrebare este aceea dacă ar trebui sau nu să reglementăm cumpărarea și deținerea acestor tehnologii, în loc să reglementăm folosirea lor.

JULIAN: Vorbim despre echipamente pentru interceptare în masă, care pot intercepta jumătate de țară sau un oraș.

JÉRÉMIE: Da. La fel ca o armă nucleară: nu poți vinde ușor o armă nucleară, iar unele țări ar putea să-și dorească să construiască una, dar au probleme. Când vorbim despre sisteme de armament, tehnologia este cea care este reglementată, nu folosirea ei. Cred că dezbaterea ar putea fi dacă aceste tehnologii ar trebui sau nu considerate ostile.

JACOB: Depinde. Când sunt arme – și nu există nici un dubiu că echipamentul pentru supraveghere este o armă în țări cum ar fi Siria sau Libia –, sunt folosite în mod special pentru a supraveghea persoane din interese politice. Compania franceză Amesys a supravegheat persoane în Regatul Unit cu tehnologie franceză care ar fi fost ilegală în Franța, și au vândut-o în cunoștință de cauză.⁵⁰

ANDY: Și nu ar face asta niciodată, nu?

JACOB: Păi, compania Amesys a fost prinsă împreună cu propriile documente interne în The Spy Files.⁵¹ Dacă e să vorbim despre lucrurile acestea în termeni de armament, trebuie să ne amintim că nu este ca și cum ai vinde unei anumite țări un camion. Este ca și cum ai vinde unei anumite țări un camion, un mecanic și o echipă care intră în camion și ia în vizor în mod selectiv oameni pe care mai apoi îi împușcă.

JULIAN: Este ca și cum ai vinde o întreagă armată de camioane.

ANDY: Este interesant că criptografia e reglementată. Există Acordul de la Wassenaar, cu aplicare internațională, care stipulează că nu poți exporta acelor țări care au fost declarate ticăloase sau, din diverse motive, problematice, tehnologie de criptare care ajută la protejarea împotriva tehnologiei de supraveghere. Dar dacă comercializezi echipament de supraveghere, *poți* să-l vinzi pe plan internațional. Pentru acesta nu există restricții la export. Iar motivul, aș spune eu, este pur și simplu acela că până și guvernele democratice au un interes propriu, și anume să controleze. Și chiar dacă faci afaceri cu țări ticăloase și le trimiți echipament de supraveghere pentru a face cu el lucruri ticăloase, tot vei avea de câștigat, pentru că vei afla lucrurile pe care le ascultă ei, lucrurile de care se tem, care sunt cei mai importanți oameni care

se opun guvernului și care organizează evenimente politice și așa mai departe. Deci vei putea prevedea evenimente viitoare, vei putea sponsoriza acțiuni și așa mai departe. Iată-ne ajunși în jocul foarte murdar reprezentat de ceea ce se întâmplă între țări, iar acesta este, de fapt, motivul pentru care sistemele de supraveghere nu sunt reglementate.

JULIAN: Aș vrea să vorbesc despre analogia dintre sistemele de supraveghere și armele de distrugere în masă. A fost o chestiune de fizică faptul că s-a putut construi bomba atomică, iar când a fost construită o bombă atomică s-a produs o schimbare geopolitică și s-a schimbat viața multor oameni – în moduri diferite, poate unele dintre ele pozitive, altele la granița apocalipsei totale. O mișcare legislativă a aplicat controale, iar până acum, aceste controale ne-au apărat de un război nuclear, excepție făcând Japonia. Dar este ușor să-ți dai seama când astfel de arme sunt folosite și când nu.

Odată cu creșterea sofisticării și cu scăderea costului supravegherii în masă din ultimii zece ani, am ajuns acum într-o situație în care populația globală se dublează o dată la aproximativ douăzeci și cinci de ani – iar capacitatea de supraveghere se dublează o dată la optsprezece luni. Curba supravegherii domină curba populației. Nu există nici o scăpare directă. Am ajuns în situația în care cu doar 10 milioane de dolari îți poți cumpăra o unitate în care să stochezi permanent interceptările în masă ale unei țări de dimensiuni medii. Deci mă întreb dacă nu cumva avem nevoie de un răspuns echivalent. Aceasta este o amenințare serioasă la adresa democrației și libertății în toată lumea și reclamă un răspuns, la fel cum amenințarea războiului atomic a reclamat un răspuns masiv, pentru a încerca să o controlăm, cât încă se mai poate.

ANDY: Eu am văzut în Libia cum mișcarea democratică a dat peste stațiile de supraveghere, a luat arhivele, a adus dovezi că

unele companii occidentale au susținut regimul lui Gaddafi în înăbușirea acțiunilor politice, iar apoi noul guvern a preluat exact acele instalații, care acum lucrează din nou la capacitate maximă.⁵² Așadar, deși sunt de acord că ar fi o idee bună să controlăm această tehnologie, sunt puțin sceptic în ceea ce privește raportul dintre interesele cetățenilor și interesele oamenilor aflați la putere. Nici nu le-aș numi neapărat guverne, pentru că oricine poate să asculte toate apelurile telefonice va putea să facă diverse chestii. Este vorba și despre prețul acțiunilor – poți beneficia mult din punct de vedere economic dacă știi ce se petrece.

JULIAN: Țările cu legislație ce reglementează interesele agențiilor principale de spionaj – agenții ca NSA în Statele Unite, GCHQ (Government Communications Headquarters) în Regatul Unit, DSD (Defence Signals Directorate) în Australia – au schimbat respectiva legislație pentru a include spionajul economic. De pildă, să spunem că dacă Australia și SUA s-ar afla în concurență într-o tranzacție cu grâu, i-ar spiona pe toți cei care sunt implicați în vânzare. Acest lucru se întâmplă deja de multă vreme, de cel puțin zece ani în mod public – dar e acceptat pentru că oamenii l-ar face oricum. A început cu vânzări de armament, caz în care ai companii ca Lockheed Martin, Raytheon și Northrup care fac comerț cu arme și care construiesc și sisteme de interceptare în masă, pentru că aceste grupuri sunt apropiate la nivel de patronaj. Au primit favoruri de la prieteni și au introdus interceptarea vânzărilor de arme sub criterii de siguranță națională. Dar acum se aplică în cazul a orice ar putea aduce beneficii unei țări din punct de vedere economic, adică la aproape orice.

JACOB: O bună analogie pe care au adus-o în discuție niște participanți la Congresul Chaos Communication, din decembrie 2011, a fost conceptul de a trata tehnologia supravegherii,

mai cu seamă tehnologia supravegherii tactice, dar și tehnologia supravegherii strategice ca pe o mină.⁵³ Cred că este o analogie puternică. Doar pentru că e posibil nu înseamnă neapărat că e și inevitabil să continuăm pe drumul acesta și nu înseamnă că trebuie să ajungem în punctul în care fiecare persoană va fi monitorizată.

Există totuși unele considerente economice care sunt împotriva noastră. De exemplu, cineva mi-a explicat felul în care funcționa sistemul norvegian de telefonie, anume acesta avea, practic, un contor care în funcție de cât de departe sunai se învârtea mai repede sau mai încet. Dar nu era legal pentru compania norvegiană de telefonie să arhiveze sau să țină un registru cu metadatele apelului efectuat, cum ar fi numărul apelat, tocmai din cauza preocupărilor legate de confidențialitate care dominau perioada celui de-al Doilea Război Mondial. Deci ar fi posibil să construim tehnologia într-o manieră care protejează confidențialitatea, dar care permite totuși o abordare de piață, ce permite totuși contribuții economice. Cu toate acestea, nu putem câștiga, de pildă, cu tehnologiile GSM (de telefonie mobilă). În momentul de față, felul în care sunt configurate aceste sisteme, nu doar în termeni de facturare, ci și în termeni de arhitectură, semnifică faptul că ele nu au confidențialitate a amplasării, nu au confidențialitate a conținutului.

JULIAN: Telefonul mobil este un instrument de urmărire care face și apeluri.

JACOB: Exact. Bunăoară, atunci când spunem că toate persoanele din Lumea a Treia sunt spionate, ce înseamnă asta în mod realist? Înseamnă că sistemele lor de telefonie, adică legătura lor cu restul lumii, sunt instrumente de spionaj în momentul în care cineva decide să se folosească de informațiile adunate în acel mod.

ANDY: Am văzut că statele africane primesc o întreagă infrastructură pentru internet, inclusiv cabluri de fibră optică și comutatoare pentru *backbone*-ul rețelei, cadou de la chinezi.

JACOB: Cadou de la ZTE sau ceva de genul ăsta?⁵⁴

ANDY: Da, și, desigur, chinezii sunt interesați de datele acelea, așa că nu trebuie să fie recompensați cu bani, ci își vor lua recompensa sub formă de date, noua monedă.

Spionajul sectorului privat

JÉRÉMIE: Supravegherea sponsorizată de stat este într-adevăr o problemă majoră, care pune sub semnul întrebării structura însăși a tuturor democrațiilor și modul în care funcționează ele, dar există și supraveghere privată și, posibil, strângere masivă de informații făcută în privat. Uitați-vă la Google. Dacă sunteți un utilizator Google standard, Google știe cu cine comunicați, pe cine cunoașteți, ce căutați, poate și orientarea voastră sexuală și credințele religioase și filosofice.

ANDY: Știe mai multe despre tine decât știi tu însuși.

JÉRÉMIE: Mai mult decât mama ta și poate chiar mai mult decât tine însuși. Google știe când ești online și când nu.

ANDY: Știi ce ai căutat acum doi ani, trei zile și patru ore? Tu nu știi; Google știe.

JÉRÉMIE: De fapt, încerc să nu mai folosesc Google, tocmai din aceste motive.

JACOB: Este un fel de Omoară-ți Televizorul în varianta secolului XXI.⁵⁵ Un protest eficient, doar că efectul de rețea împiedică protestul tău să funcționeze.⁵⁶ Omoară-ți televizorul, omule.

JÉRÉMIE: Păi nu este un protest, este mai degrabă felul meu personal de a vedea lucrurile.

ANDY: Am văzut niște filmări foarte frumoase cu oameni care-și aruncau televizoarele din clădiri de câte trei etaje.

JÉRÉMIE: Nu e vorba doar de supravegherea sponsorizată de stat, e vorba despre chestiunea confidențialității, de felul în care datele sunt administrate de terți și de măsura în care oamenii au cunoștință despre ceea ce se face cu datele. Eu nu folosesc Facebook, deci nu știu prea multe despre el. Dar acum, cu Facebook-ul, poți vedea comportamentul unor utilizatori care sunt foarte încântați să ofere orice fel de date personale, și poți să-i învinovățești că nu știu care este limita dintre privat și public? Acum câțiva ani, înainte de tehnologiile digitale, oamenii care aveau o viață publică erau fie în show-business, fie în politică sau în jurnalism, iar acum fiecare are posibilitatea unei vieți publice prin simpla apăsare a unui buton de distribuire. A „distribui“ înseamnă a face ceva public, înseamnă a acorda accesul către acele date restului lumii – și, desigur, când vezi adolescenți care postează poze cu ei beți sau mai știu eu ce, s-ar putea ca ei să nu vadă lucrurile în acest fel, anume că înseamnă tot restul lumii, poate pentru o perioadă foarte, foarte lungă. Facebook funcționează ca afacere prin estomparea granițelor dintre confidențialitate, prieteni și publicitate. Și îți și stochează datele, atunci când tu crezi că sunt destinate doar prietenilor tăi și oamenilor care-ți sunt dragi. Deci oricare e gradul în care dorești să îți fie publice datele, de fiecare dată când postezi ceva pe Facebook trimiți mai întâi datele acelea către Facebook, iar apoi ei acordă accesul la ele anumitor utilizatori.

JULIAN: Chiar și limita dintre guvern și corporații este estompată. Dacă ar fi să ne uităm la expansiunea din sectorul antreprenorial militar în Occident în ultimii zece ani, vedem că NSA,

care era cea mai mare agenție de spionaj din lume, avea în registrele sale zece contractori principali cu care lucra. Acum doi ani avea peste 1 000. Deci se estompează granița dintre ceea ce reprezintă guvern și ceea ce reprezintă sectorul privat.

JÉRÉMIE: Și se poate susține că agențiile de spionaj ale SUA au acces la toate datele stocate de Google.

JULIAN: Dar chiar au.

JÉRÉMIE: Și la toate datele Facebook, deci într-un fel Facebook și Google ar putea fi prelungiri ale acestor agenții.

JULIAN: Tu ai vreo somație Google, Jake? A primit cumva Google o somație pentru a preda informațiile referitoare la contul tău Google? În cazul WikiLeaks s-au trimis somații la Dynadot, compania din California unde se înregistrează numele de domeniu și unde este înregistrat și wikileaks.org. Erau somații care făceau parte din investigația secretă a Marelui Juriu împotriva WikiLeaks și în care se cereau arhivele financiare, arhivele de autentificări etc. și pe care Google i le-a dat.⁵⁷

JACOB: *Wall Street Journal* a relatat că Twitter, Google și Sonic.net, trei servicii pe care le folosesc sau pe care le-am folosit în trecut, au primit fiecare câte o notificare 2703(d), tipul acesta neobișnuit de somație secretă.⁵⁸

JULIAN: În temeiul PATRIOT Act?

JACOB: Nu. Aici este vorba, în esență, de Legea Comunicațiilor Arhivate. *Wall Street Journal* spune că fiecare dintre aceste servicii pretinde că guvernul vrea metadatele, iar guvernul a declarat că are dreptul de a face acest lucru fără mandat. Există un proces în curs de desfășurare despre dreptul guvernului de a-și ține tacticile

secrete, nu doar față de public, ci și față de tribunale. Citesc *Wall Street Journal* și am aflat și eu ca toți ceilalți.

JULIAN: Deci Google s-a pus bine cu guvernul SUA în cadrul investigației împotriva WikiLeaks, când guvernul a emis o somație pentru arhivele tale – nu o somație normală, ci această somație specială, pentru spionaj. Dar apăruse știrea, undeva la începutul lui 2011, că Twitter ar fi primit mai multe somații, emise de același Mare Juriu, dar Twitter s-a luptat în instanță pentru a putea anunța oamenii ale căror conturi erau somate – pentru a fi ridicată interdicția de a notifica părțile vizate. Nu am un cont de Twitter, deci eu nu am primit una, dar numele meu și cel al lui Bradley Manning erau pe toate somațiile, figurând în dreptul informației căutate. Jake, tu aveai un cont de Twitter, deci Twitter a primit o somație referitoare la tine. Și Google a primit o somație, dar nu s-a luptat în instanță pentru a o face publică.⁵⁹

JACOB: Așa se pare. Așa am citit în *Wall Street Journal*. S-ar putea să nu am nici măcar voie să fac referire la acest lucru decât în legătură cu *Wall Street Journal*.

JULIAN: E cumva din cauză că aceste ordine au o clauză de păstrare forțată a tăcerii? Lucrul ăsta a fost declarat neconstituțional, nu-i așa?

JACOB: Poate că nu. În cazul procesului Twitter, e știut public faptul că am pierdut moțiunea de suspendare în care am spus că cedarea acestor date guvernului ar cauza daune ireparabile, din cauză că nu le va mai putea uita odată ce le-a primit. Ei au zis: „Ei bine, moțiunea de suspendare este respinsă, Twitter trebuie să cedeze datele“. Acum am făcut recurs în instanță, în special în cazul ținerii secrete a evidenței sentințelor – și pot să vorbesc despre asta –, dar, după cum arată lucrurile acum, curtea a afirmat

că nu te poți aștepta la confidențialitate pe internet, când destăinuie în mod voluntar informații unor terți, și, apropo, toată lumea e o terță persoană pe internet.

JULIAN: Chiar dacă organizații ca Facebook și Twitter spun că informația va rămâne privată.

JACOB: Sigur. Iar aceasta este estomparea granițelor dintre stat și corporații. Poate lucrul cel mai important pe care trebuie să ni-l amintim este acesta, că NSA și Google au un parteneriat în securitate cibernetică din rațiuni de apărare națională.

ANDY: Orice ar însemna securitate cibernetică în acest context. E un termen foarte larg.

JACOB: Încearcă să scoată totul de sub Legea Libertății Informației și să țină totul secret. Apoi, guvernul SUA afirmă de asemenea că are dreptul de a trimite somații administrative care au o autoritate mai mică decât un mandat de percheziție, somații în cazul cărora terții au interdicția de a te anunța în legătură cu ele, iar tu nu ai nici un drept de a ataca asta în instanță, pentru că sunt implicați în mod direct doar terții, iar terții nu au nici un temei constituțional pentru a-ți proteja datele.

JULIAN: Terții fiind Twitter sau Facebook sau ISP*-ul tău.

JACOB: Sau oricine. Au spus că există, în cazul confidențialității bancare sau al formării unui număr de telefon, o legătură directă, de tipul *one-to-one* [unul-către-unul]. Prin simplul fapt că folosiți telefonul, divulgați numărul, de bunăvoie, companiei respective de telefonie. Știați asta, nu? Folosind telefonul spuneți în mod evident: „Nu am nici o așteptare de confidențialitate” atunci când formați acele numere. Există o conexiune încă și mai puțin

* „Internet Service Provider” – *Furnizor de internet* (n.tr.)

explicită cu aparatul. Oamenii nu înțeleg cum funcționează internetul – nu înțeleg nici cum funcționează rețelele de telefonie –, dar tribunalele au hotărât de fiecare dată că așa stau lucrurile, iar în procesul nostru Twitter de până acum, despre care din păcate nu pot vorbi pentru că nu trăiesc într-o țară liberă, se spune, în esență, același lucru.⁶⁰

Este nebunie curată să ne imaginăm că predăm toată informația personală acestor companii, iar companiile au devenit, în esență, o poliție secretă privatizată. Iar – în cazul Facebook – există chiar supraveghere democratizată. În loc să fie plătiți, cum făcea Stasi în Germania de Est, oamenii sunt recompensați ca cultură – acum și-o trag. Anunță despre prietenii lor: „Hei, cutare s-a logodit“; „A, cutare s-a despărțit“; „A, acum știu pe cine să sun“.

ANDY: Au fost oameni care au reușit să facă presiuni ca Facebook să le dezvăluie toate datele arhivate despre ei, conform Legii Europene a Protecției Datelor, și cantitatea cea mai mică a fost de 350 MB, cea mai mare a fost în jur de 800 MB.⁶¹ Lucrul interesant este că astfel a ieșit la iveală structura bazei de date a Facebook-ului. De fiecare dată când intri pe Facebook se înregistrează adresa ta de IP și toate celelalte lucruri, fiecare click pe care-l faci, fiecare accesare și numărul de accesări ale unei pagini, astfel încât să poată să-și dea seama dacă îți place sau nu și așa mai departe. Dar acest lucru a dezvăluit că identificatorul-cheie al structurii bazei de date este cuvântul „target“. Nu-i numesc pe acești oameni „abonați“ sau „utilizatori“ sau mai știu eu cum, îi numesc „ținte“, la care ai putea spune: „Bine, e un termen din marketing“.

JULIAN: Dar era privat pe plan intern.

ANDY: Da, dar ar putea fi ținte și într-un sens militar, sau ar putea fi ținte într-un sens de spionaj. Deci ține doar de contextul în care sunt folosite datele.

JULIAN: Da. Asta face ca lucrul ăsta să fie atât de înspăimântător.

ANDY: Mie mi se pare foarte util lucrul ăsta. Obişnuiam să spunem, în cazul Facebook-ului, că utilizatorul nu este de fapt consumatorul. Utilizatorul Facebook este de fapt produsul, iar adevăratul consumator sunt companiile de publicitate. Este explicația cea mai puțin paranoică, cea mai inofensivă despre ceea ce se petrece.

Dar problema este că nu poți învinovăți o companie că se supune legilor unei țări. Este normal să fie așa, și este o infracțiune dacă companiile nu se supun legilor țării. Deci e destul de greu să spui că „Hei, se supun legii“. Ce fel de acuzație mai e și asta?

JACOB: Nu, e un lucru cu care trebuie să fiu în dezacord în afirmația asta. Dacă construiești un sistem care înregistrează totul despre o persoană și știi că trăiești într-o țară cu legi care vor obliga guvernul să predea aceste date, poate că nu ar trebui să construiești un astfel de sistem. Iar asta este diferența dintre o abordare de tipul „confidențialitate-prin-politică“ și una de tipul „confidențialitate-prin-construcție“ în crearea unor sisteme sigure. Dacă încerci să transformi oamenii în ținte și știi că trăiești într-o țară care face asta în mod explicit, atunci dacă Facebook și-ar instala serverele în Libia lui Gaddafi sau în Siria lui Assad ar fi un lucru foarte neglijent. Și totuși, nici una dintre scrisorile de siguranță națională care au fost emise, cred, anul trecut sau acum doi ani nu aveau nimic de-a face cu terorismul. Vreo 250 000 au fost folosite pentru orice altceva, numai nu pentru a lupta împotriva terorismului.⁶² Deci știind că aceasta este realitatea, aceste companii au o răspundere etică serioasă care izvorăște din faptul că construiesc aceste sisteme și că au luat practic decizia economică de a-și vinde utilizatorii. Iar ăsta nici măcar nu e un lucru tehnic. Nu are nici o legătură cu tehnologia, e vorba despre economie.

Au decis că este mai important să colaboreze cu statul și să-și vândă toți utilizatorii și să le încalce confidențialitatea și să facă parte dintr-un sistem al controlului – să fie plătiți pentru că fac parte din cultura supravegherii, că fac parte din cultura controlului – decât să-i opună rezistență, așa că au devenit o parte integrantă. Sunt complici și răspunzători.

ANDY: Răspunderea etică nu e o chestiune chiar atât de importantă în zilele noastre, nu-i așa?

Combaterea supravegherii totale cu legile fizicii

JÉRÉMIE: O întrebare care ar putea fi ridicată acum ar fi: care este soluția, fie pentru utilizatorul individual, fie pentru societate în întregul ei? Există soluții tehnice – servicii descentralizate, ca fiecare să-și găzduiască propriile date, ca toată lumea să aibă încredere în furnizori apropiați lor, care să-i ajute cu servicii de criptare a datelor, și așa mai departe. Iar apoi există opțiunea diverselor politici pe care le-am discutat. Nu sunt sigur că în acest moment putem răspunde la întrebarea dacă una dintre cele două abordări este mai bună. Cred că trebuie să dezvoltăm cele două abordări în paralel. Trebuie să avem software liber, pe care să-l înțeleagă toată lumea, pe care toată lumea să-l poată modifica și pe care fiecare să îl poată examina pentru a fi sigur de ceea ce face. Cred că software-ul liber este una din bazele pentru o societate online liberă, pentru a avea oricând posibilitatea de a controla mașina și de a nu lăsa mașina să te controleze pe tine. Trebuie să avem o criptografie puternică, pentru ca atunci când vrei ca datele tale să fie citite doar de tine, nimeni să nu le mai poată citi. Avem nevoie de instrumente de comunicare ca Tor sau Cryptophone, pentru a putea comunica doar cu oamenii cu care vrei să comunici. Dar se prea poate ca puterea statului și puterea companiilor

să depășească întotdeauna puterea unor experți în calculatoare ca noi și capacitatea noastră de a elabora și distribui tehnologiile astea. De asemenea, s-ar putea să avem nevoie, în timp ce vom construi tehnologiile astea, de legi și de instrumente care să fie în mâinile cetățenilor, pentru a putea controla ceea ce se face cu tehnologia – chiar dacă nu întotdeauna în timp real – și pentru a-i putea sancționa pe cei care folosesc tehnologia într-un mod neetic și într-un mod care încalcă confidențialitatea cetățenilor.

JULIAN: Vreau să mă uit la ceea ce văd ca fiind o diferență între perspectiva cypherpunk în Statele Unite și perspectiva europeană. Al Doilea Amendament al SUA este dreptul de a purta armă. Chiar recent am văzut o filmare, realizată de un prieten în SUA, despre dreptul de a purta armă, iar deasupra unui magazin de armament era un semn pe care scria „Democracy, Locked and Loaded“ [Democrația, încărcată și gata să tragă]. Acesta este modul în care te asiguri că nu ai regimuri totalitare – oamenii sunt înarmați, iar dacă sunt destul de enervați își iau pur și simplu armele și preiau controlul cu forța. O întrebare interesantă e dacă argumentul acesta mai e încă valabil, din cauza diferențierii tipurilor de arme care a avut loc în ultimii treizeci de ani. Ne putem aminti de afirmația că crearea de coduri – furnizarea de coduri criptografice secrete pe care guvernul nu le poate spiona – este în realitate o formă de muniție. Am dus acest mare război în anii '90 pentru a încerca să aducem criptografia la îndemâna tuturor și l-am câștigat în mare parte.⁶³

JACOB: În Occident.

JULIAN: Am câștigat în Occident, iar acum se află în fiecare browser, deși poate că acum este supravegheată și subminată în diverse moduri.⁶⁴ Chestiunea este că nu poți avea încredere că guvernul va implementa politicile pe care spune că le implementează, așa

că trebuie să asigurăm noi instrumentele de bază, instrumentele criptografice pe care le controlăm noi, ca un fel de uz de forță, în sensul că, dacă cifrarea merge bine, guvernul nu va putea, oricât de tare ar încerca, să aibă acces la comunicațiile noastre în mod direct.

JACOB: Puterea aproape oricărei autorități moderne este derivată din violență sau din amenințarea cu violență. Trebuie să acceptăm faptul că în cazul criptografiei violența nu va putea rezolva niciodată o problemă de matematică.

JULIAN: Exact.

JACOB: Acesta este lucrul important. Nu înseamnă că nu poți fi torturat, nu înseamnă că nu vor putea să-ți instaleze microfoane în casă sau să o submineze în vreun fel, dar înseamnă că dacă găsesc un mesaj criptat nu contează dacă au forța autorității în spatele oricărei acțiuni pe care o fac, tot nu vor putea rezolva acea problemă de matematică. Acesta însă este un lucru care nu este evident pentru oamenii care nu sunt tehnici, și trebuie să facem în așa fel încât să devină evident. Dacă am putea rezolva acele probleme de matematică ar fi o altă poveste și, sigur, dacă cineva ar fi în stare să le rezolve, guvernul ar fi acela.

JULIAN: Dar se întâmplă ca o caracteristică a realității în care trăim, la fel precum cea reprezentată de faptul că poți construi bombe atomice, să fie aceea că există unele probleme matematice care pot fi elaborate și pe care nici cel mai puternic stat nu le poate rezolva. Cred că lucrul acesta a fost foarte atrăgător pentru libertarii din California, și nu numai, care au crezut în idealul acesta al „democrației încărcate și gata să tragă”, pentru că aveau aici un mod foarte intelectual de a o face – câțiva indivizi ținând piept întregii forțe a celei mai puternice puteri din lume prin intermediul criptografiei.

Așadar există o proprietate a universului care se află de partea confidențialității, fiindcă unii algoritmi de criptare nu pot fi spărți de nici un guvern, niciodată. Mai sunt alții despre care știm că sunt extrem de greu de spart, chiar și pentru NSA. Știm aceasta pentru că chiar ei recomandă antreprenorilor armatei SUA să folosească acești algoritmi pentru protejarea comunicațiilor strict secrete ale armatei, iar dacă ar exista vreo modalitate de a-i sparge ar fi fost găsită repede de ruși sau de chinezi, cu consecințe grave pentru cel care a luat decizia de a recomanda un cifru nesecurizat. Deci cifrurile sunt acum destul de bune, avem destulă încredere în ele. Din păcate nu poți avea deloc încredere în aparatul cu care le folosești, deci asta este o problemă. Dar lucrul ăsta nu duce la interceptare în masă; duce la urmărirea computerelor unor anumiți oameni. Este foarte greu să securizezi un computer dacă nu ești un expert în securizare. Dar criptografia poate rezolva problema interceptării în masă, iar problema interceptării în masă este cea care pune în pericol civilizația globală. Nu urmărirea individuală este amenințarea.

Cu toate acestea, sunt de părere că avem de-a face cu forțe economice și politice uriașe, după cum a spus și Jérémie, iar rezultatul cel mai probabil este că eficiența naturală a tehnologiilor de supraveghere comparată cu numărul oamenilor va duce la faptul că încetul cu încetul vom deveni o societate polițienească totalitară și globală – prin totalitară vreau să spun una a supravegherii totale – și că probabil ultimii oameni liberi rămași în viață vor fi cei care înțeleg cum să folosească criptografia pentru a se apăra împotriva acestei supravegheri complete, totale, precum și unii oameni care au ieșit complet din sistem, neoluddiți care s-au ascuns în peșteri sau popoare tribale tradiționale care nu au nici unul din avantajele unei economii moderne, deci capacitatea lor de a juca vreun rol este foarte limitată. E evident că oricine poate să stea departe de internet, dar atunci le este foarte dificil

să aibă vreo influență. Făcând lucrul acesta își elimină posibilitatea de a fi influenți. Este aceeași situație cu telefoanele mobile; poți alege să nu ai un telefon mobil, dar îți reduci influența. Nu e o cale înainte.

JÉRÉMIE: Dacă privești lucrurile dintr-o perspectivă de piață, sunt convins că există o piață a confidențialității care a rămas în mare parte neexplorată, așa că poate va exista un stimulent economic pentru unele companii de a crea instrumente care le vor acorda utilizatorilor posibilitatea individuală de a-și controla datele și comunicațiile. Poate că aceasta este o modalitate în care putem rezolva această problemă. Nu sunt sigur dacă ar putea funcționa de una singură, dar aceasta s-ar putea întâmpla și s-ar putea să nu o știm încă.

JULIAN: Criptografia va fi peste tot. Este lansată de toate marile organizații, care tind să se transforme într-o rețea de orașe-stat. Dacă e să ne gândim la căile de comunicare de pe internet – tranzacții financiare transnaționale rapide, organizații transnaționale, interconexiuni între subdiviziuni ale organizațiilor –, toate acele fluxuri de informații trec prin canale de comunicație nesecurizate. Este asemenea unui organism fără piele. Există organizații și state care ajung să nu se mai distingă unele de altele – fiecare rețea de influență mondială concurând pentru avantaj –, iar comunicațiile lor sunt expuse oportuniștilor, concurenților statelor și așa mai departe. Așa că se contruiesc rețele noi, peste internet, rețele virtuale private, iar confidențialitatea lor e garantată de criptografie. Aceasta este o bază a puterii industriale care împiedică interzicerea criptografiei.

Dacă ar fi să ne uităm la telefonul Blackberry, de exemplu, acesta are un sistem de criptare inclus care poate fi folosit în interiorul rețelei Blackberry. Research in Motion, compania canadiană

care-l operează, poate descifra traficul utilizatorilor și are centre de date cel puțin în Canada și în Regatul Unit, iar în acest fel alianța anglo-americană a spionajului poate avea acces la comunicațiile Blackberry către Blackberry din lumea întreagă. Dar companiile mari folosesc acest principiu în moduri mai sigure. Guvernele occidentale au fost de acord cu lucrul acesta până în momentul în care s-a extins de la corporații la indivizi, iar apoi am văzut exact aceleași reacții politice ostile pe care le-am văzut în Egipt, sub guvernul lui Mubarak.⁶⁵

Cred că singura apărare eficientă împotriva distopiei supravegherii care se apropie este cea în care iei singur măsuri pentru a-ți proteja confidențialitatea, deoarece oamenii care au capacitatea de a intercepta totul nu au nici o motivație pentru a-și limita acțiunile. O analogie istorică ar putea-o reprezenta felul în care au învățat oamenii că ar trebui să se spele pe mâini. A fost nevoie de formularea teoriei microbilor și de popularizarea ei și de instalarea paranoiei despre răspândirea bolilor prin niște chestii invizibile de pe mâini, pe care nu le puteai vedea așa cum nu poți vedea interceptarea în masă. Odată ce a fost înțeles fenomenul, producătorii de săpun au creat produse pe care oamenii le-au consumat pentru a-și calma frica. Este necesar ca frica să pună stăpânire pe oameni astfel încât aceștia să înțeleagă problema și abia apoi se va crea destulă cerere pentru ca ea să fie rezolvată.

Există o problemă și de partea opusă a ecuației, și anume faptul că programele care pretind că sunt securizate, care pretind că conțin criptografie sunt deseori escrocherii, din cauză că criptografia este complexă, iar escrocheria poate fi ascunsă în complexitate.⁶⁶

Deci oamenii vor trebui să se gândească la acest lucru. Singura întrebare este în care dintre cele două feluri se vor gândi la el. Fie se vor gândi că „Trebuie să fiu atent la ce spun, trebuie să mă conformez” tot timpul, în fiecare interacțiune, fie se vor gândi

că „Trebuie să-mi însușesc mici componente ale acestei tehnologii și să-mi instalez lucruri care să mă protejeze astfel încât să-mi pot exprima liber gândurile și să comunic liber cu prietenii mei și cu oamenii la care țin“. Dacă oamenii nu adoptă modalitatea a doua, vom avea o corectitudine politică universală, pentru că oamenii se vor autocenzura chiar și atunci când vor vorbi cu prietenii lor cei mai apropiați și se vor elimina din postura de actori politici.

Internetul și politica

JÉRÉMIE: Este interesant să observi puterea hackerilor – „hacker“ în sensul primar al cuvântului, nu în cel de infractor. Hackerul este un iubitor al tehnologiei, cineva căruia îi place să înțeleagă cum funcționează tehnologia, nu pentru a fi captivul tehnologiei, ci pentru a o face să funcționeze mai bine. Bănuiesc că la vârsta de cinci sau șapte ani ați avut și voi șurubelniță și ați încercat să deschideți un aparat pentru a vedea cum este pe dinăuntru. Asta înseamnă să fii un hacker, iar hackerii au construit internetul din mai multe motive, inclusiv pentru că era o distracție, și l-au dezvoltat și au dat internetul tuturor. Companii ca Google sau Facebook au văzut oportunitatea de a-și construi modele de afaceri bazate pe preluarea datelor personale ale utilizatorilor. Dar totuși putem observa o formă de putere în mâinile hackerilor. Ceea ce mă interesează în principal în ultima vreme este faptul că acești hackeri capătă putere, chiar și în arenele politice. În SUA s-a propus această legislație SOPA (Legea Opririi Pirateriei Online) și PIPA (Legea pentru Protecția IP-urilor) – reglementări violente ale drepturilor de autor care, în esență, acordă Hollywoodului puterea de a ordona oricărei companii de internet să restricționeze accesul și să cenzureze internetul.⁶⁷

JULIAN: Și blocaje financiare asemenea celei la care este supusă WikiLeaks.⁶⁸

JÉRÉMIE: Exact. Ceea ce s-a întâmplat în cazul WikiLeaks din cauza companiilor bancare devenise metoda standard pentru a lupta cu pirații ticăloși ai drepturilor de autor care au omorât Hollywoodul și așa mai departe. Și am fost martorii acestui tumult uriaș creat pe internet de societatea civilă – și nu doar în Statele Unite, fenomenul nu ar fi funcționat dacă doar cetățenii SUA s-ar fi ridicat împotriva SOPA și PIPA. Au participat oameni din toată lumea, iar hackerii s-au aflat în centrul lucrurilor și au furnizat celorlalți instrumente pentru a înlesni participarea în dezbateră publică.

JULIAN: Pentru a ajuta la construirea campaniei.

JÉRÉMIE: Nu cumva pe Tumblr, sau pe un alt site de genul ăsta, poți să-ți lași pe prima pagină numărul de telefon, urmând apoi să fii sunat și pus în legătură cu Congresul? Și puteai pur și simplu să începi să vorbești cu cineva și să spui „Da, ce faceți voi e o tâmpenie“.

JACOB: Internetul a fost folosit pentru autoapărare.

JÉRÉMIE: Eu cred că noi, ca hackeri, avem o răspundere față de instrumentele pe care le construim și pe care le distribuim restului lumii, și putem fi martorii începutului eficienței cu care această răspundere poate fi pusă în practică când o folosim colectiv. Astăzi, Uniunea Europeană se află în procesul dezbaterii ACTA – ACTA (Acordul Comercial de Combatere a Contrafacerii) este un tratat multinațional care stă la baza legilor SOPA și PIPA.⁶⁹ Tocmai m-am întors de la Parlamentul European unde noi, ca indivizi, indivizi bărboși și mirositori, am dictat unei comisii parlamentare. Le-am arătat articole în regulile de procedură ale

Parlamentului European pe care păreau că le văd pentru prima oară și le-am spus cum să procedeze și am câștigat votul cu 21 la 5, lucru care a marginalizat raportorul britanic într-un colț îndepărtat. Aceasta este o parte foarte mică dintr-o mică chestiune procedurală pe calea spre înfrângerea acordului ACTA, acest acord global monstruos care a fost creat în secret pentru a circumscrie democrația însăși. Dar ar fi posibil să omorâm acest monstru, în calitate de cetățeni – ușor, cu instrumentele internetului, cu listele de e-mailuri, cu wiki-urile, cu platformele de chat ale IRC* etc. –, și cred că putem fi martorii trecerii internetului de la copilărie la adolescență și ai felului în care poate fi el folosit de societatea întreagă pentru a încerca să facă lucrurile să se schimbe. Cred că este de o importanță uriașă faptul că noi, hackerii, suntem aici cu cunoștințele noastre tehnice pentru a ghida oamenii și pentru a le spune: „Ar trebui să folosiți această tehnologie care vă permite controlul asupra confidențialității datelor voastre, în loc de Facebook sau Google“, și că cele două se articulează împreună destul de bine – sau ar putea să se articuleze împreună destul de bine. Este un pic de optimism aici.

JULIAN: Jake, vorbind despre această radicalizare politică a tineretului de pe internet, tu ai călătorit în toată lumea, mai cu seamă în ultimii doi ani, vorbind despre Tor, vorbind cu oameni care vor anonimitate, care vor confidențialitate față de propriul guvern, și trebuie să fi văzut acest fenomen în țări diferite. Este un lucru semnificativ?

JACOB: Cu siguranță. Exemplul canonic la care mă gândesc imediat este vizita în Tunisia. Am fost în Tunisia după căderea regimului lui Ben Ali și am vorbit despre Tor la un curs de informatică la care au participat și niște oameni foarte tehnici de la

* Internet Relay Chat – comunicare instantanee pe internet (n.tr.)

universitate, iar cineva a ridicat mâna și a spus: „Dar cum rămâne cu oamenii ticăloși?” Iar apoi a trăncănit întruna despre cei Patru Călăreți ai Apocalipsei Informatice – spălarea de bani, drogurile, terorismul și pornografia infantilă. „Cum rămâne cu oamenii ticăloși?” Aceste patru lucruri sunt aduse tot timpul în discuție și spectrul lor este folosit pentru a ataca tehnologiile de apărare a confidențialității, pentru că e evident că trebuie să eliminăm aceste patru grupuri. Așa că i-am întrebat pe cei aflați la curs: „Cine a văzut vreodată pagina Ammar 404?”, care este pagina de cenzură introdusă de regimul Ben Ali înainte și în timpul revoluției, pentru a bloca accesul. Fiecare persoană din clasă a ridicat mâna, inclusiv profesorul, în afară de cea care pusese întrebarea. Și m-am uitat la fata care pusese această întrebare și i-am zis: „Privește la toți oamenii din jurul tău. Adică la toți colegii tăi. Crezi tu cu adevărat că a meritat ca toate persoanele din clasă să fie asuprite pentru a lupta împotriva acelor lucruri?” Și a zis: „De fapt, am să ridiș și eu mâna”.

S-a vorbit ceva mai mult de atât, dar în esență oamenii care văd lucrurile în context își dau seama care este situația reală. Asta schimbă situația în mod dramatic. Iar asta se întâmplă în toată lumea, tot timpul – dar de obicei se întâmplă mai târziu, adică oamenii se uită înapoi și își dau seama că ar fi putut folosi acea tehnologie, își dau seama că „A, da, se pare că nu e vorba doar de ticăloși pentru că, de fapt, eu sunt ticălosul dacă încerc să vorbesc în mod liber despre ceva, iar cuiva de la putere nu-i place ce am de spus despre asta”. Și poți observa că are loc o deșteptare.

Dar e fals să spui că s-a întâmplat doar în ultimii doi ani. Îmi pare rău să-ți fac asta, Julian, dar tu ești o parte a radicalizării generației mele. Eu sunt un cypherpunk de generația a treia, dacă am număra așa. Munca pe care ați depus-o tu și Ralf Weinmann la sistemul de fișiere *rubberhose* a fost, în parte, cea care m-a inspirat pe mine să lucrez la sisteme de criptare. Sistemul criptografic

de fișiere pe care l-am creat, numit M.A.I.D., a fost o reacție la lucruri cum ar fi legea *Regulation of Investigatory Powers* [Reglementarea Puterilor Investigatoare] din Regatul Unit, prin care, în esență, statul a decis că soluția la criptografie este reglementarea negativă și că îți poate fi luată parola.⁷⁰ Desigur, în cazul lui Julian, când au creat asta a fost din cauză că regimurile opresive torturau oamenii pentru o parolă, deci trebuia să poți da mai multe parole pentru a face față torturii lor. Sistemul meu criptografic, M.A.I.D., a fost creat pentru un sistem legal în care acuzatul are dreptul de a păstra tăcerea, dar poate dovedi, dacă este constrâns, că spune adevărul, fără a încălca confidențialitatea. Când am văzut activitatea lui Julian mi-am dat seama că poți folosi tehnologia pentru a da oamenilor obișnuiți puterea de a schimba lumea. Întorcându-mă înapoi la vechea listă de e-mailuri Cypherpunk cu Tim May, unul dintre membrii ei fondatori, și citind vechile postări ale lui Julian în lista Cypherpunk, realizez că asta e ceea ce a determinat o întreagă generație de oameni să devină mai radicali, pentru că oamenii și-au dat seama că nu mai erau atomizați, că puteau petrece ceva timp scriind un software care ar putea duce la emanciparea a milioane de oameni.⁷¹

Există însă niște consecințe neintenționate ale dezvoltării acestui lucru, pentru că cei care au creat Google nu și-au propus să creeze Google, să creeze cea mai mare mașinărie de supraveghere care a existat vreodată. Dar de fapt asta s-a creat, iar de îndată ce oamenii vor începe să-și dea seama de acest lucru, vor începe să trimită acele Scrisori de Siguranță Națională, nu?

JÉRÉMIE: Cred că sunt trei lucruri de importanță crucială în ceea ce ai spus.

JACOB: Doar trei?

JÉRÉMIE: Printre altele.

ANDY: Ok, lăsați-mă să-l adaug pe cel de-al patrulea, bine?

JACOB: Dar încă nici nu știi care sunt acelea trei.

JÉRÉMIE: Văd trei elemente-cheie legate între ele. Nu spun că ele ar trebui luate separat, dar unul dintre ele îl reprezintă regimurile autoritare și puterile pe care le au regimurile autoritare într-o epocă a tehnologiilor digitale. În cazul regimului lui Ben Ali – iar astăzi lucrul acesta este evident în foarte multe alte regimuri –, poți decide ce anume pot să afle oamenii sau cu cine pot comunica. Lucrul acesta presupune o putere enormă și ar trebui să ne împotrivim lui, iar internetul – un internet liber – este un instrument prin care să ne împotrivim lucrului acestuia. Un alt element-cheie este construcția unor instrumente și tehnologii mai bune, tehnologii care pot încerca să ocolească probleme precum cenzura, dar, în mare, instrumente care să facă parte din infrastructura care să ne ajute să răsturnăm dictatorii. Iar încă o problemă este discursul politic pe care l-ai evocat, cei Patru Călăreți ai Apocalipsei Informatice, pretextele care sunt folosite în fiecare zi de către politicieni în mass-media – „Vom muri cu toții din cauza terorismului? Avem nevoie de Patriot Act“; „Cei care distribuie pornografie infantilă sunt peste tot“; „Internetul este plin de pedo-naziști, deci e nevoie de cenzură“.

JACOB: Pedo-naziști?

JÉRÉMIE: Pedo-naziști, da – pedo-nazi.com e rezervat deja. „Artiștii vor muri de foame și nu va mai exista cinema, așa că trebuie să dăm Hollywoodului puterea de a cenzura internetul“, și așa mai departe. Cred că și în acest caz internetul este un instrument, un antidot împotriva discursului politic. Discursul politic se bazează pe sentimentalism și pe un cadru temporal al prezentării informației extrem de scurt – informația apare și dispare după

douăzeci și patru de ore și este înlocuită de informație nouă. Cu ajutorul internetului, am senzația că suntem în procesul de a construi ceea ce eu numesc timpul internetului. Din cauză că marele internet nu uită niciodată, putem construi dosare pe parcursul anilor, în fiecare zi, și putem elabora, putem analiza. Asta e ceea ce am făcut în ultimii trei ani cu ACTA. Și, din nou, WikiLeaks ne-a inspirat, fiindcă prima versiune a ACTA care a fost scursă a fost scursă la WikiLeaks în 2008.⁷²

JULIAN: Da, am cules-o noi.

JÉRÉMIE: Și am scurs și noi două versiuni. În ultimii trei ani au existat cinci versiuni ale textului pe care le-am putut lua și spune, paragraf cu paragraf, rând cu rând, că cutare face lucrul ăsta, aici e industria care cere cutare lucru, și am putut să implicăm experți legali și experți tehnologici și să construim un discurs politic diferit de oficialul „Avem nevoie de ACTA pentru a salva cultura și a salva copiii de medicamentele false” și alte afirmații de genul ăsta. Așa că ne-am construit propriul program politic mulțumită timpului internetului, prin analiză precisă, muncă grea, conectând oamenii unii cu alții pentru a participa la lucrul acesta.

JULIAN: E adevărat, și cred că viziunea aceasta asupra ACTA a cucerit publicul.

JÉRÉMIE: Până acum e bine.

JULIAN: Aceasta cred că va fi viziunea istorică, dar, în spatele cortinei, acest așa-numit Acord Comercial de Combatere a Contrafacerii, care a fost propus de industria drepturilor de autor a SUA, a fost de fapt folosit într-o mulțime de tratate bilaterale, pentru a încerca să se creeze un nou regim internațional privitor la ce este legal și ce nu este legal în ceea ce privește publicarea și la mecanismele care pot fi folosite pentru a împiedica oamenii

de la publicarea anumitor lucruri. Standardizează o versiune mai dură a legii DMCA din Statele Unite (Legea privind Drepturile de Autor Digitale), care spune că dacă trimiți cuiva o scrisoare prin care îi ceri să dea jos un lucru de pe internet, e obligat să-l dea jos, și există un fel de proces de două săptămâni în care poate veni cu contraargumente și așa mai departe, dar din cauză că e scump pentru orice ISP să aibă de-a face cu contraargumente, îl coboară imediat, și-i permit autorului sau celui care l-a urcat să se lupte singur. Efectul acestui lucru a fost destul de pronunțat în Statele Unite, în ceea ce privește ștergerea unei cantități mari de conținut. Scientology a abuzat de aceasta pentru a scoate efectiv mii de înregistrări video de pe YouTube.⁷³

Deci hai să presupunem că ACTA a fost respinsă în Parlamentul European, și chiar cu succes, cel puțin versiunea aceasta. Dar manifestările principale ale ACTA par să se petreacă oricum – a existat dezbateră democratică, ACTA a fost demonizată în sfera publică, am ieșit învingători în discursul politic, dar în spațiile cortinei au fost elaborate tratate bilaterale secrete care obțin același rezultat, tot ce au făcut a fost să submineze procesul democratic. De exemplu, WikiLeaks a intrat în posesia noului acord de comerț liber între UE și India și l-a publicat, acord care include bucăți mari din ACTA.⁷⁴ Acest lucru s-a întâmplat cu mai multe alte acorduri și legislații. Capul ACTA ar putea foarte bine să fie tăiat, dar corpul se va despica în câteva bucăți, iar fiecare dintre ele își va croi drum către alte lucruri, către ordinea internațională sub forma acestor tratate internaționale. Deci puteți avea victoriile democratice care au loc în public, la suprafață, dar dedesubt lucrurile se fac oricum. Lucru care cred că arată că nu reforma politică sau legislativă este răspunsul; deși nici nu poți da adversarului o lovitură liberă, pentru că atunci va urgenta lucrurile. Deci e important să controlăm fenomenul în diverse moduri, la fel cum controlăm ACTA. Îi încetinim

manifestarea. Dar nici măcar o victorie în parlament în ceea ce privește legislația nu oprește această activitate care se desfășoară în strat mai profund.

JACOB: Un lucru care cred că trebuie subliniat este faptul că Roger Dingledine, unul dintre creatorii Tor, despre care aş spune că mi-e un fel de mentor și care mi-a dat mult de gândit în ceea ce privește împiedicarea cenzurii și anonimitatea online, vorbește despre cum, de exemplu, un firewall nu are succes doar din punct de vedere tehnic – și este important să înțelegi tehnologia din spațele său dacă vrei să contruiești o tehnologie care să i se opună –, dar are succes și din punct de vedere social. Oamenii care luptă împotriva acordului ACTA folosesc tehnologie, iar tehnologia le permite să stea pe poziții, dar în realitate cea pe care este important să o înțelegem în cazul acesta este forța reprezentată de oamenii obișnuiți, iar vorbăria tehnică nu este lucrul important. Ceea ce contează este ca oamenii să se implice în toată povestea asta și s-o schimbe cât încă au puterea să o facă, așa că aspectul uman este, de fapt, partea cea mai importantă. WikiLeaks a publicat documente care permit aceasta, iar distribuirea de informație este importantă, dar și persoanele care preiau acea informație importantă și o transmit contează. Pentru că există cel puțin argumentul că mulți dintre noi trăim într-o democrație, că suntem liberi, că ar trebui să fie așa încât să fim guvernați prin consimțământ. Și astfel, dacă toată lumea înțelege ce se petrece și dacă găsim că ceea ce se petrece nu este un lucru consimțit de noi, atunci este foarte greu să se continue și să se treacă legile și să se facă totul fără consimțământul celor guvernați.

JÉRÉMIE: Este vorba despre creșterea costurilor politice ale luării unor decizii proaste pentru cei care le iau, și putem face acest lucru în mod colectiv, cu un internet liber, atâta vreme cât îl avem la îndemână.

JACOB: Dar ai putea să o faci și fără internet, pentru că am avut – în istorie – societăți libere înainte de internet, doar că era mai costisitor din punct de vedere economic, era mai dificil în anumite privințe, iar asta este motivul pentru care mișcarea peer-to-peer este atât de importantă.⁷⁵

ANDY: Punctul numărul patru este, cred eu, acela că arhitectura descentralizată a sistemelor este un lucru fundamental, care trebuie pus de asemenea în mâinile poporului, pentru că acum există acest cloud computing centralizat.⁷⁶

JULIAN: Facebook este complet centralizat. Twitter este complet centralizat. Google este complet centralizat. Toate în Statele Unite; toate sub controlul celor care controlează forța coercitivă. La fel ca procesul de cenzură care a început după ce WikiLeaks a publicat Cabledgate, când Amazon ne-a scos site-ul de pe serverele lor.⁷⁷

ANDY: Iar cloud computing stimulează din punct de vedere economic companiile să aibă o modalitate mai ieftină de a procesa datele în așa-numitele centre de date, conduse de corporații americane, lucru care înseamnă că aduc datele în jurisdicția SUA, la fel ca în cazul companiilor de plăți și așa mai departe.

JULIAN: Există o tendință în contextul trecerii la cloud computing care este destul de îngrijorătoare. Există îngrămădiri de servere într-un singur loc, pentru că este mai eficient să standardizezi astfel controlul asupra mediului înconjurător, să standardizezi sistemul de plată. Este o tehnică competitivă din cauză că acumularea de servere într-un singur loc e mai ieftină decât răspândirea lor. Majoritatea comunicației care se face pe internet, în afară de streaming-ul de video, se face între server și server, deci dacă pui serverele mai aproape unul de celălalt este mai ieftin. Rezultatul îl reprezintă aceste mari stupuri de servere comunicante. Are sens

ca Google, de exemplu, să-și plaseze serverele lângă marii furnizori de conținut, sau invers, pentru că paginile sunt indexate de Google pentru a putea fi căutate. Deci există în SUA clădiri uriașe care sunt pur și simplu pline de servere de la diverse companii. Astea sunt locurile în care NSA își instalează unele dintre punctele de colectare a interceptărilor în masă. Internetul nu ar putea exista fără această centralizare, nu din cauză că este imposibil din punct de vedere tehnologic, ci doar din cauză că este pur și simplu mult mai eficient să fie centralizat. În competiția economică, versiunea centralizată câștigă.

ANDY: Deși e foarte important să înțelegem punctul de vedere arhitectural – infrastructurile centralizate fac să fie foarte ușoare controlul central și abuzul de putere –, e de asemenea ca și cum ai distruge micul supermarket de la colț printr-un concept centralizat de comerț cu amănuntul.

JULIAN: Mergându-se către o multinațională uriașă, cum este Safeway.

ANDY: Da, la fel cum s-a întâmplat cu shopping-ul. Este foarte important să păstrăm o abordare descentralizată a infrastructurii. Când eram membru al ICANN – Internet Corporation for Assigned Names and Numbers [Corporația Internet pentru Alocare de Nume și Numere], care creează și reglementează numele de domenii de pe internet, am aflat ceva de la Vince Cerf, cel care a inventat, cel puțin în parte, protocolul TCP/IP, protocolul fundamental de comunicație pe internet. Avea obiceiul să spună: „Știi, un lucru bun despre guverne e că nu sunt niciodată singulare, sunt întotdeauna la plural“. Deci, chiar și printre guverne, există acelea care vor să aibă propria rază de acțiune descentralizată, și chiar în interiorul guvernelor există diferite facțiuni care se luptă între ele. Acesta este lucrul care ne va salva în final de Big

Brother, pentru că vor fi prea mulți care vor dori să fie Big Brother și se vor lupta între ei.

JULIAN: Nu cred, Andy. Cred că au existat la un moment dat elite naționale care concureau una cu cealaltă, și că acum acestea se asociază unele cu altele și se despart de propriul popor.

ANDY: Se asociază, în sensul ăsta ai dreptate – și nu sunt nici eu atât de sigur că ne va salva lucrul ăsta –, dar există o șansă să ne păstrăm identitatea. Trebuie să rămânem fideli propriei noastre infrastructuri, acesta este lucrul important de învățat aici – că dacă vrem să ne opunem statului polițienesc, unui unic Big Brother, trebuie să învățăm ce înseamnă lucrul ăsta, dacă este într-adevăr o asociere de state centrale care își spun: „Hei, dacă ne unim am putea câștiga și mai mult“. Și trebuie să știm care ne este rolul aici – rolul nostru este să rămânem descentralizați, să avem propria noastră infrastructură, să nu ne bazăm pe cloud computing și alte tâmpenii, ci să avem sistemul propriu.

JULIAN: Dar s-ar putea să avem această dominație a tehnicii. Dacă este adevărat că e mai ușor să folosești Twitter decât să-ți creezi propriul Twitter; dacă este adevărat că e mai ușor să folosești Facebook decât DIASPORA sau vreo altă alternativă; dacă este adevărat că cloud computing e mai ieftin, atunci aceste tehnici și servicii vor fi dominante.⁷⁸ Nu e vorba despre a spune că trebuie să ne creăm propriile servicii locale, pentru că aceste servicii locale nu vor putea fi competitive, pur și simplu, și vor fi folosite doar de o minoritate mică de oameni. Avem nevoie de ceva mai bun decât a spune că trebuie să avem o variantă pentru săraci a Facebook-ului și să ne așteptăm ca oamenii să o folosească.

ANDY: Păi, revenind la Biserica Romano-Catolică, ne întoarcem la timpurile în care există un singur editor principal de carte, din

cauză că Amazon caută să controleze întreg lanțul de furnizare de cărți electronice, deci trebuie să ne păstrăm capacitatea proprie de tipărire și publicare. S-ar putea să pară puțin exagerat, dar am văzut ce pot face aceste companii dacă nu vor, fie ele, fie agențiile guvernamentale de care depind în jurisdicția lor, ca unele lucruri să se întâmple. Și cred că pasul următor va trebui să fie, evident, că vom avea nevoie de propriii noștri bani, astfel încât, chiar dacă nu le place că susținem proiecte ca WikiLeaks sau mai știu eu ce, noi vom avea modul nostru propriu de a o face, fără să ne bazăm pe o infrastructură centrală care aparține unei singure jurisdicții.

JÉRÉMIE: Aș vrea să fiu de acord cu ceea ce spune Andy. Cred că arhitectura contează și că acest lucru este crucial pentru tot ceea ce susținem. Dar acesta este un mesaj pe care avem răspunderea de a-l comunica publicului, pentru că noi îl înțelegem, ca hackeri, ca tehnicieni care construiesc internetul zilnic și se joacă cu el. Și poate că aceasta este o modalitate de a câștiga inimile și mințile tinerelor generații. Din cauza asta cred că războaiele drepturilor de autor sunt esențiale, pentru că, prin intermediul tehnologiilor de tipul peer-to-peer, de când cu Napster în 1999, oamenii au înțeles – au prins ideea – că distribuind fișiere între indivizi...

JULIAN: Ești un infractor.

JÉRÉMIE: Nu, construiești o cultură mai bună.

JULIAN: Nu, ești un infractor.

JÉRÉMIE: Țasta e discursul, dar dacă construiești o cultură mai bună pentru tine însuși, toată lumea va folosi Napster.⁷⁹

ANDY: Istoria rasei umane și istoria culturii sunt istoria copierii gândurilor, a modificării lor și a procesării lor ulterioare, și dacă numești asta furt, ești la fel ca toți cinicii.

JÉRÉMIE: Exact, exact! Cultura e făcută pentru a fi distribuită.

JULIAN: Păi începând cu anii '50, în Occident am avut o cultură industrială. Cultura noastră a devenit un produs industrial.

JÉRÉMIE: Cred că ce facem noi aici e să îi dăm apă la moară, fiindcă joacă rolul de avocat al diavolului și o face foarte bine.

JACOB: Eu nu mușc momeala. E evident că e o tâmpenie.

JÉRÉMIE: Este o tâmpenie. În discursul politic se numește furt, dar vreau să spun că toată lumea care a folosit Napster în 1999 a devenit un fan al muzicii și s-a dus la concerte și a spus tuturor „Trebuie să-i ascuți pe oamenii ăștia, trebuie să te duci la concertul cutare“ și așa mai departe. Deci oamenii au avut un exemplu practic despre cum tehnologia peer-to-peer a descentralizat arhitectura. De fapt, Napster era puțin centralizat pe vremea aceea, dar a însămânțat ideea unei arhitecturi descentralizate. Toată lumea avea un exemplu concret despre cum arhitectura descentralizată aduce un bine societății, iar când este vorba despre distribuirea culturii este la fel ca atunci când este vorba despre distribuirea cunoașterii. Distribuirea cunoașterii este lucrul despre care vorbim atunci când discutăm despre a ocoli cenzura sau despre a ne croi drum prin discursul politic pentru a construi un sistem democratic mai bun și pentru a îmbunătăți societatea.

Așadar, avem exemple în care serviciile descentralizate și distribuția între indivizi fac ca lucrurile să fie mai bune, iar contraexemplul este avocatul diavolului pe care-l joacă Julian, când vine o industrie și spune: „Oh, lucrul ăsta este furt și omoară pe toată lumea, omoară actorii, omoară Hollywoodul, omoară cinematografia, omoară pisicuțe și totul“. Au câștigat bătlia în trecut, iar acum s-ar putea să câștigăm noi bătlia ACTA. Și trebuie să fim în dezacord din nou cu avocatul diavolului pe care l-a jucat

Julian înainte. ACTA a fost cel mai bun exemplu de ocolire a democrației de până acum, în care s-a cântat în strună parlamentului și instituțiilor internaționale, s-a cântat în strună opiniei publice, iar pe ușa din dos s-au impus măsuri inacceptabile. Dacă reușim să respingem asta, atunci vom stabili un precedent, vom avea oportunitatea să impunem o agendă de lucru pozitivă, să spunem „ACTA s-a terminat, acum hai să facem ceva care e cu adevărat în favoarea publicului“. Și lucrăm în direcția asta, iar unii membri ai Parlamentului European înțeleg acum că atunci când indivizii distribuie lucruri, când distribuie fișiere fără profit, nu ar trebui să meargă la închisoare, nu ar trebui pedepsiți. Cred că dacă reușim să facem asta avem șanse bune să arătăm restului lumii că distribuirea cunoașterii, distribuirea informației fac ca lucrurile să fie mai bune, că trebuie să promovăm lucrul ăsta, și nu să-l atacăm și că orice încercare – fie ea legislativă sau din partea unui dictator sau a unei companii – de a lovi în capacitatea noastră de a distribui informații și a distribui cunoaștere într-o manieră descentralizată trebuie atacată. Punct. Cred că putem face ca această atitudine să ia avânt.

JULIAN: Cum rămâne cu dezbaterea PIPA/SOPA în Statele Unite? Aceasta este o legislație nouă, propusă în Congres pentru ca industriile SUA să creeze embargouri financiare și blocaje ale internetului în numele industriilor americane.

JACOB: A fost creată anume pentru a ataca WikiLeaks și lucruri care țin de WikiLeaks sau asemănătoare cu WikiLeaks.

JULIAN: Blocada bancară împotriva noastră a fost menționată anume în Congres ca un instrument eficace.⁸⁰

JÉRÉMIE: Și era vorba să se dea acest instrument Hollywoodului.

JULIAN: Așa că am organizat o mare campanie comunitară împotriva acestui lucru și într-un final Google și Wikipedia și mulți alții s-au alăturat campaniei. Dar nu mi-am spus: „Ok, e foarte bine, am câștigat bătălia“. M-am speriat de moarte, din cauză că Google s-a văzut dintr-odată ca jucător politic, și nu doar ca distribuitor, și a simțit acea putere uriașă, fantastică asupra Congresului.

JÉRÉMIE: Google era doar o parte mică din coaliția anti-SOPA și PIPA.

JACOB: Da, dar stai puțin, că Tumblr, cred, a avut un impact și mai mare decât a avut Google.

ANDY: Tumblr și Wikipedia și mii de acțiuni individuale, acțiuni foarte mici de care poate nu ați auzit niciodată, au avut un impact. Mii de astfel de acțiuni se aflau în paralel – mergând în aceeași direcție –, iar asta este, din nou, acțiune politică descentralizată. Este o mișcare politică descentralizată la care am fost martori. S-ar putea ca Google să fi fost doar cel mai mare actor pe care l-ai observat între ceilalți.

JULIAN: Ei bine, asta a spus Congresul că ar fi observat.

JACOB: Eu am o mică problemă cu ceea ce a spus Jérémie înainte, pentru că, în esență, promovezi ideea unei avangarde politice. Nu cred că era intenția ta să faci lucrul ăsta, dar l-ai făcut și vreau doar să te opresc în loc, pentru că mișcarea peer-to-peer se împotrivesc în mod explicit unei avangarde politice. Ea reprezintă ideea că suntem cu toții egali și că putem distribui între noi; am putea furniza servicii diferite sau am putea furniza funcționalitate diferită. Ross Anderson mi-a spus odată: „Când m-am alăturat mișcării peer-to-peer, acum cincizeci de ani“, ceea ce mi s-a părut un început fantastic de propoziție. Mi-a explicat că vrea să se asigure că nu vom dez-inventa niciodată presa de tipar. Pentru

că pe măsură ce începem să centralizăm serviciile, pe măsură ce începem să centralizăm controlul asupra sistemelor de informație, în realitate chiar începem să dez-inventăm presa de tipar, în sensul că *Enciclopedia Britannica* nu mai tipărește cărți, ci doar imprimă CD-uri – dacă nu ai un computer cu scop generalist care poate citi acele CD-uri, nu ai acces la acea cunoaștere. Acum, ceea ce se întâmplă în cazul *Enciclopediei Britannica* nu contează, pentru că avem Wikipedia și avem mult alt material. Dar nu cred că suntem pregătiți, ca societate.

ANDY: Nu sunt sigur că Wikipedia este atât de bună ca resursă, dacă e să facem o comparație. Nu am încredere în nici o pagină de acolo pe care să nu o fi rescris eu.

JACOB: Dar *Enciclopedia Britannica* nu e diferită. Este doar o sursă între multe altele, iar ceea ce contează este verificarea datelor. Tot ceea ce vreau să spun este că nu ar trebui să promovăm ideea unei avangarde, din cauză că este foarte periculoasă.

JULIAN: Stai puțin, de ce? Și eu sunt un fel de avangardist. Care e problema cu ei?

JÉRÉMIE: Eu nu vorbesc despre avangarde, spun doar că avem instrumente noi la îndemână. Vorbeam despre presa de tipar. Un alt vizionar, un prieten de-al meu, Benjamin Bayart, poate mai puțin cunoscut în afara lumii francofone, a spus: „Presa de tipar a învățat poporul să citească; internetul a învățat poporul să scrie”.⁸¹ Acesta e un lucru foarte nou, aceasta este o posibilitate nouă, ca toată lumea să poată scrie și să se poată exprima.

ANDY: Da, dar filtrarea devine și mai importantă în zilele noastre.

JÉRÉMIE: Sigur, pentru că toată lumea vorbește și multă lume spune tâmpenii. După cum îți va spune academicianul și activistul

Larry Lessig și, cred eu, atâția alți profesori, învățăm oamenii cum să scrie, dar când studenții își predau lucrările, peste nouăzeci și nouă la sută dintre ele sunt de rahat, dar cu toate acestea îi învățăm să scrie.⁸² Așadar, desigur, oamenii spun tâmpenii pe internet – e evident. Dar faptul de a putea să folosești această posibilitate pentru a te exprima în public te face cu timpul din ce în ce mai elocvent în felul tău de a vorbi, din ce în ce mai capabil să participi la discuții complexe. Și toate fenomenele pe care le descriem sunt construite pe principiul unei complexități pe care trebuie să o divizăm în părți mici pentru a putea să o înțelegem și să o dezbatem cu calm. Nu este vorba despre o avangardă politică, este vorba despre a canaliza prin sistemul politic această nouă posibilitate de a ne exprima pe care o avem la îndemână, de a ne împărtăși gândurile, de a participa la distribuirea cunoașterii fără să fim membri ai unui partid politic, ai unei companii media sau ai oricărei alte structuri centralizate de care aveai nevoie în trecut pentru a putea să te exprimi.

Internetul și economia

JULIAN: Aș vrea să mă uit la trei libertăți fundamentale. Când l-am intervievat pe șeful Hezbollah, Hassan Nasrallah...

JACOB: Acolo unde e blestematul ăla de atac cu drone? Ce se întâmplă acolo?

JULIAN: Păi are și el un fel de arest la domiciliu, pentru că nu poate să părăsească locul secret în care se află.

JACOB: Nu sunt sigur că aș face comparația asta. Te rog, nu face comparația asta.

JULIAN: E discutabil dacă Hezbollah are ingredientele unui stat – a devenit oare un stat? Acesta este un lucru menționat în telegramele ambasadei SUA, și anume că Hezbollah și-a construit propria rețea de cabluri de fibră optică în sudul Libanului.⁸³ Deci are cele trei ingrediente principale ale unui stat – are controlul forței armate într-o anumită regiune, are o infrastructură de comunicații pe care o controlează și are o infrastructură financiară pe care o controlează. Și ne putem gândi la acestea ca la trei libertăți fundamentale. Libertatea de mișcare, libertatea fizică de mișcare – posibilitatea de a călători dintr-un loc în altul, fără ca armata să se mobilizeze împotriva ta. Ne putem gândi la libertatea

de gândire, și la libertatea de comunicare, care e inclusă în libertatea de gândire – dacă ești pus în pericol pentru că vorbești în public, singurul mod de a-ți apăra dreptul de a comunica este să comunici în privat. Și, în sfârșit, libertatea interacțiunii economice, care se cuplează, de asemenea, ca libertatea de comunicare, cu confidențialitatea interacțiunii economice. Așa că hai să vorbim despre aceste idei, care s-au dezvoltat în mișcarea cypherpunk încă din anii '90, referitoare la încercarea de a furniza această foarte importantă a treia libertate, care este libertatea interacțiunii economice.

JÉRÉMIE: Dar de ce ai avea nevoie doar de trei libertăți? În Carta Europeană a Drepturilor Fundamentale sunt mai multe.

JULIAN: Confidențialitatea devine importantă fie dintr-o perspectivă comunitară, adică ai nevoie de confidențialitate pentru a comunica liber și a gândi liber, fie ai nevoie de ea, în vreun fel sau altul, pentru interacțiunile tale economice. Deci cred că există mai multe libertăți derivate, dar acestea – primele trei pe care le-am numit – sunt libertățile fundamentale din care derivă toate celelalte libertăți.

JÉRÉMIE: Păi există o definiție legală a libertății fundamentale.

JULIAN: Dar am citit Carta UE și pot să-ți spun că este un dezastru total în ceea ce privește consensul.

JÉRÉMIE: Da, OK, și s-au făcut presiuni și au reușit să bage și proprietatea intelectuală în Carta UE.

JULIAN: Tot felul de chestii pur și simplu demente.

ANDY: Cred totuși că există un lucru cu care să fim de acord, și anume acela că sistemul monetar, infrastructura economică de schimb monetar, este foarte proastă în momentul de față.

Și chiar cineva care are doar un cont de eBay va fi într-un totu de acord cu lucrul ăsta, pentru că ceea ce face Paypal, ceea ce fac Visa și MasterCard, este să pună lumea, *de facto*, într-o situație de monopol. Un lucru foarte interesant, aflat tot din telegramele WikiLeaks, este acela că guvernul Rusiei a încercat să negocieze o modalitate prin care plățile Visa și MasterCard efectuate de cetățeni ruși, pe teritoriul Rusiei, să fie procesate în Rusia, iar Visa și MasterCard au refuzat.⁸⁴

JULIAN: Da, puterea combinată a ambasadei Americii și a Visa a fost suficientă pentru a împiedica până și Rusia să-și creeze propriul sistem de plată prin card pe teritoriul său.

ANDY: Ceea ce înseamnă că până și plățile efectuate de cetățeni ruși, la magazine rusești, vor fi procesate prin centre de date americane. Deci guvernul SUA va avea controlul jurisdicțional, sau cel puțin informații din interior.

JULIAN: Da, deci când Putin iese să-și ia o Cola, peste treizeci de secunde se știe la Washington.

ANDY: Iar asta, desigur, este o situație foarte nemulțumitoare, indiferent dacă-mi place de SUA sau nu. Este pur și simplu un lucru foarte periculos să ai o locație centrală în care sunt stocate toate plățile, pentru că facilitează tot felul de întrebări ale acelor date.

JACOB: Unul dintre lucrurile fundamentale de care și-au dat seama activiștii cypherpunk este că arhitectura definește într-adevăr situația politică, deci dacă ai o arhitectură centralizată, chiar dacă o controlează cei mai cumsecade oameni din lume, ea va atrage ticăloși, iar acei ticăloși vor face lucruri cu puterea lor pe care cei care au proiectat-o nu le-ar face. Și este important să ne dăm seama că lucrul acesta se aplică și în cazul banilor.

JULIAN: La fel ca puțurile de țiței din Arabia Saudită, blestemul țițeiului.

JACOB: Oriunde ne-am uita, mai cu seamă în cazul sistemelor financiare, observăm că, de fapt, chiar dacă oamenii au cele mai bune intenții, nu contează. Arhitectura este adevărul. Este adevărul internetului în ceea ce privește comunicațiile. Așa-numitele sisteme de interceptare legală, ceea ce nu e decât un mod drăguț de a spune spionarea oamenilor...

JULIAN: Este un eufemism, interceptarea legală.

JACOB: Absolut, la fel ca omorul legal.

ANDY: Sau tortura legală.

JACOB: Ați auzit despre atacurile legale cu dronă împotriva cetățenilor americani ale președintelui SUA, Obama? Când l-a omorât pe fiul de șaisprezece ani al lui Anwar al-Awlaki în Yemen, a fost omor legal, sau *targeted killing*, cum i-au spus ei [asasinare la comandă].⁸⁵ Așa-numita interceptare legală este același lucru – pui pur și simplu legal înaintea tuturor cuvintelor și dintr-odată, din cauză că o face statul, devin legitime. Dar, de fapt, arhitectura statului este cea care le permite să facă lucrul ăsta, arhitectura legilor și arhitectura tehnologiei, tot așa cum e și arhitectura sistemelor financiare.

Ceea ce mișcarea cypherpunk și-a dorit să facă este să creeze sisteme care să ne permită să ne plătim unul pe altul într-un mod cu adevărat liber, în care să nu fie posibil să se intervină. Cum este moneda chaumiană, care este o monedă electronică proiectată după specificațiile lui David Chaum, cel care a creat eCash (o monedă electronică complet anonimă), deși ai putea să spui că e mai centralizată decât ar fi necesar. Ideea este să creezi o monedă anonimă, diferită de Visa/MasterCard, care este o monedă ce poate

fi urmărită. Deși e construită în jurul unei autorități centrale, moneda chaumiană folosește protocoale criptografice inventate de David Chaum, pentru a asigura tranzacții anonime.⁸⁶

JULIAN: Deci practic cash electronic fără, să zicem, numere de serie pe bancnote.

JACOB: Sau numere de serie care-ți permit să stabilești că este o monedă valabilă, dar nu-ți permit să știi neapărat că Julian i-a făcut o plată lui Andy, sau să știi care a fost suma.

JÉRÉMIE: Este de fapt recrearea cash-ului în lumea digitală.

JULIAN: Crearea unei monede electronice este un lucru important tocmai din cauză că controlul asupra mijlocului de schimb este unul dintre cele trei ingrediente ale unui stat, după cum spuneam referitor la Hezbollah. Dacă sustragi statului monopolul asupra mijloacelor de interacțiune economică, sustragi unul dintre cele trei ingrediente principale ale statului. În modelul statului ca mafie, unde statul este o organizație care asigură protecția sub amenințarea pedepsei violente, statul scutură oamenii de bani în toate modurile posibile. Controlarea fluxului de monedă este importantă pentru creșterea venitului de către stat, dar este de asemenea importantă pur și simplu pentru a controla ceea ce fac oamenii – promovând un lucru, inhibând un altul, interzicând complet o anumită activitate sau o organizație, sau interacțiunile dintre organizații. Așadar, de exemplu, în cazul extraordinarei blocaje financiare împotriva WikiLeaks, nu piața liberă e cea care a decis să blocheze WikiLeaks, pentru că nu există o piață liberă – legislația guvernului a numit anumiți actori financiari regi și nu permite intrarea pe piață a altora. Libertatea economică a fost încălcată de către un grup de elită care poate influența atât legislația, cât și principiile după care operează aceste bănci.⁸⁷

ANDY: Aceasta este marea problemă nerezolvată a lumii electronice în ziua de astăzi, și mă întristează să o spun. Două companii de credit, ambele cu o infrastructură de plată electronică cu baza în SUA – ceea ce înseamnă accesul la date în jurisdicția SUA –, controlează majoritatea plăților cu cardul de credit de pe planetă. O companie precum Paypal, care e de asemenea sub jurisdicție SUA, aplică politici SUA, fie că asta înseamnă blocarea vânzării de trabucuri cubaneze de către magazine germane online sau blocarea plăților către WikiLeaks în jurisdicții din afara SUA. Asta înseamnă că guvernul SUA are accesul la date și opțiunea de a impune controale asupra plăților din întreaga lume. Deși cetățenii americani ar putea susține că aceasta este cea mai bună democrație posibilă, pentru cetățenii europeni lucrul acesta e ridicol.

JULIAN: În lumea tradițională am avut o anumită libertate de mișcare, nu prea mare în unele cazuri.

JACOB: Ești sigur, Julian? Am sentimentul că libertatea ta de mișcare este un exemplu elocvent despre cât de liberi suntem cu adevărat.

JULIAN: Păi nu, Regatul Unit a anunțat că va pune 100 000 de oameni pe an în situația mea.⁸⁸ Deci cred că e colateral într-o anumită măsură.

JACOB: Țsta e motivul pentru care fondatorii țării mele au împușcat oameni din Marea Britanie. Avem un motiv bine întemeiat pentru care i-am împușcat pe brianici. Iar el încă există și astăzi. Tirania există.

JÉRÉMIE: Hai să nu facem remarci personale.

ANDY: Ceea ce SUA, țara ta, fac în momentul de față, este să privatizeze închisorile administrate anterior de guvern și să

negocieze cu companiile private care administrează aceste închisori contracte ce garantează o rată de ocupare de nouăzeci la sută.⁸⁹ Păi ce-i asta? Țsta e capitalismul împins la absurd.

JULIAN: Există mai mulți oameni în închisorile SUA decât erau în Uniunea Sovietică.

JACOB: Aceasta e eroarea de judecată în care, din cauză că eu protestez împotriva unui lucru greșit, tu poți sugera că aș face parte dintr-un lucru la fel de greșit. Nu vreau să sugerez că Statele Unite ar fi perfecte. Cred că Statele Unite sunt destul de faine în multe privințe, dar mai cu seamă în ceea ce privește retorica Părinților Fondatori.

JULIAN: Retorica Părinților Fondatori s-a aflat într-o clară disoluție în ultimii zece ani.

JACOB: Trebuie să nu pierdem din vedere faptul că o mare parte din percepția despre retorica Părinților Fondatori este mitologie și că ar trebui să fim atenți să nu-i idolatrizăm. Deci da, desigur. Tot ceea ce am vrut să spun, prin comentariul meu despre tirania britanică și despre situația în care se află Julian, este că acest lucru este în realitate o chestie culturală. Aici intră în scenă societatea și aici societatea este foarte importantă, și este foarte dificil ca tehnologia să înlocuiască acest lucru. Iar chestiunile financiare sunt lucrul cel mai periculos de care să te ocupi. Există un motiv bine întemeiat pentru care cel care a creat o altă monedă electronică, Bitcoin, a făcut-o anonim. Nu vrei să fii cel care inventează prima monedă electronică de succes.⁹⁰

JULIAN: Băieții care au inventat e-gold au sfârșit prin a fi urmăriți penal în SUA.⁹¹

JACOB: Este foarte frustrant.

JULIAN: Aș vrea să mă întorc la aceste trei libertăți fundamentale: libertatea de a comunica, libertatea de mișcare și libertatea interacțiunii economice. Dacă ar fi să ne uităm la trecerea la internet a societății noastre globale, când am făcut acea trecere, libertatea de mișcare personală a rămas neschimbată, practic. Libertatea de a comunica a sporit într-o manieră uluitoare în anumite privințe, în sensul că acum putem comunica cu mult mai mulți oameni; pe de altă parte, s-a și degradat într-o manieră uluitoare, pentru că nu mai există confidențialitate, iar astfel comunicarea noastră poate fi spionată, și chiar este spionată și stocată și, în consecință, poate fi folosită împotriva noastră. Și astfel, acea interacțiune elementară pe care o avem în mod fizic cu oamenii este degradată și ea.

ANDY: Confidențialitatea este posibilă, dar are un cost.

JULIAN: Interacțiunile noastre economice au avut de suferit aceleași consecințe. Căci în cazul unei interacțiuni economice tradiționale, cine știe de ea? Cei care te-au văzut că ai mers la piață. Dar acum, cine știe despre interacțiunea ta economică? Dacă cumperi ceva de la vecinul tău cu cardul Visa, lucru pe care, într-o societate tradițională de piață, ai fi putut să-l faci aproape complet în privat, cine știe acum despre asta?

JACOB: Toată lumea.

JULIAN: Toată lumea știe. Distribuția de date se face între toate marile puteri occidentale, toate știu despre asta și stochează datele pentru totdeauna.

ANDY: Julian, ceea ce spui tu nu este fals, dar nu sunt sigur că putem face cu adevărat distincție între libertatea de a comunica și libertatea interacțiunii economice, din cauză că internetul, așa cum îl avem astăzi, este infrastructura pentru interacțiunile

noastre sociale, economice, culturale, politice, pentru toate interacțiunile noastre.

JACOB: În mod cert libertatea de mișcare.

ANDY: Oricare ar fi arhitectura comunicațiilor, banii sunt doar biți. Este doar folosire a internetului. Deci dacă sistemul economic este bazat pe infrastructura electronică, atunci arhitectura infrastructurii electronice spune ceva despre cum are loc fluxul monetar, despre cum este el controlat, cum este centralizat și așa mai departe. Poate că internetul nici nu a fost gândit, în primele zile ale existenței sale, ca o infrastructură pentru orice, dar logica economică spune: „Păi, este mai ieftin să facem cutare lucru cu internetul“. Băncile și companiile de carduri de credit aveau bancomate dinainte, cu interfețe X.25, ceea ce constituia o rețea separată acum zece sau douăzeci de ani, iar acum totul este TCP/IP pentru că e mai ieftin.⁹² Deci arhitectura tehnologiei devine o cheie-din cauza că afectează toate celelalte arii, iar de asta avem nevoie pentru a regândi cu adevărat lucrurile, în sensul că dacă vrem o modalitate economică descentralizată de a ne administra plățile, trebuie să preluăm infrastructura.

JACOB: Bitcoin este în esență o monedă electronică.

ANDY: Fără inflație.

JACOB: Tinde să o facă într-o manieră descentralizată, deci în loc să ai Sistemul Federal de Rezervă Monetară, ai o mână de oameni în toată lumea care hotărăsc de comun acord care e realitatea și care e moneda lor curentă.

JULIAN: Și există și programe de calculator care facilitează lucrul acesta.

JACOB: Vreau să explic asta într-o manieră care nu este tehnică. Este o monedă electronică care este mai degrabă o marfă decât

o monedă, în sensul că oamenii stabilesc câți euro are un Bitcoin. Deci este un pic ca aurul în acest sens și mai există și costul așa-numitei extracții a Bitcoin-ului, unde operezi o căutare pe un computer pentru a găsi un Bitcoin, și ideea este că există o complexitate a calculelor și că ea este legată de valoarea lucrului. Deci în termeni non-tehnici este o modalitate ca eu să-î trimit bani lui Julian fără ca Andy să fie în stare să intervină sau să oprească tranzacția. Există și unele probleme, însă – nu este în realitate o monedă anonimă, iar acesta este un lucru nesatisfăcător, în opinia mea.

JULIAN: Bitcoin este un hibrid foarte interesant, pentru că deținătorii de conturi sunt în întregime anonimi și pentru că poți să-ți faci un cont oricând dorești, dar tranzacțiile întregii economii Bitcoin sunt complet publice. Și așa funcționează ea; trebuie să fie așa, pentru ca toată lumea să poată verifica dacă o tranzacție s-a produs, dacă contul expeditor are acum mai puțini bani, iar cel destinat are mai mulți. Aceasta este una dintre puținele modalități în care poți permite funcționarea unui sistem monetar online care nu necesită un server central, fiindcă acesta ar putea fi o țintă atrăgătoare pentru controlul coercitiv. Dar distribuția este cea care este cu adevărat inovatoare în cazul Bitcoin, și algoritmi care permit distribuția, în sensul că nu te încrezi anume în vreuna dintre părțile rețelei bancare Bitcoin, ca să-i spunem așa. Ci încrederea este distribuită. Iar funcționarea regulamentară a sistemului nu se face prin legi sau reguli sau controale, se face prin dificultatea calculului criptografic prin care trebuie să treacă fiecare parte a rețelei pentru a dovedi că face ceea ce susține că face. Deci funcționarea regulamentară a unui „sistem bancar” onest bazat pe Bitcoin este integrată în arhitectura sistemului. Calculul se traduce în costuri de electricitate pentru fiecare ramură a băncii Bitcoin, deci fraudarea poate să aibă un cost, în

termenii prețului la electricitate. Lucrurile sunt stabilite în așa fel încât munca necesară comiterii unei fraude să presupună costuri de electricitate mai mari decât beneficiul economic care rezultă din ea. Este foarte inovativ, nu pentru că aceste idei nu ar fi fost explorate înainte (ele au existat timp de douăzeci de ani, pe hârtie), ci pentru că Bitcoin a găsit echilibrul perfect și a adăugat o idee foarte inovativă despre cum să atingi un adevărat consens global cu privire la tranzacțiile economiei Bitcoin, chiar pornind de la prezumția că multe bănci sunt frauduloase și că oricine ar putea fonda una.

Desigur, la fel ca oricare altă monedă, trebuie să cumperi această monedă cu altceva, cu muncă, sau Bitcoin-ul poate fi schimbat cu o altă monedă – există grupări de schimb valutar care fac asta. Mai sunt și alte limitări. Are o perioadă de achitare a plății de circa zece minute – e nevoie de aproximativ zece minute de activitate de calcul între transferul de monedă și asigurarea de către a doua parte că există un consens global asupra efectuării tranzacției. Este exact ca o monedă fizică, așa că are toate problemele legate de furt pe care le are moneda fizică. Are de asemenea și toate avantajele: odată ce ai primit banii, poți fi sigur că ai fost plătit, cecul nu poate fi anulat, banca nu-l poate retrage. Relațiile de forță coercitivă le taie legăturile. Pe de altă parte, trebuie să păzești bine moneda. Aceasta este, cred eu, cea mai mare problemă a sa. Dar este destul de ușor să adaugi mai multe straturi deasupra, să construiești servicii de împuternicire legală prin care să-ți stochezi banii într-un server care este conceput anume pentru a-i păstra în siguranță și pentru a-i asigura împotriva furtului.

JACOB: Ce este interesant e că dacă cei care au creat Bitcoin ar fi stabilit ca Tor să fie folosit în mod obligatoriu de toată lumea, astfel încât să nu-ți creezi un cont, ci să creezi niște identificatoare criptografice, ar fi fost posibil, dacă totul ar fi trecut prin Tor ca

structură internă a întregului sistem, să ai confidențialitate a locației, chiar dacă ai fi avut totuși identificatori folosiți pe termen lung care te identificau ca să-ți poți lega tranzacțiile unele de altele.

JÉRÉMIE: Fără să intrăm în chestiuni de ordin tehnic, am putea cădea cu toții de acord că Bitcoin are la bază concepte excelente, dar și unele neajunsuri. Are o natură deflaționistă, pentru că banii tind să dispară de pe Bitcoin. Deci nu poate funcționa pe termen lung, dar introduce concepte care pot fi îmbunătățite. E probabil versiunea 0.7 sau 0.8 acum.

JACOB: Este ca și cum ai reinventa David Chaum.⁹³

ANDY: Bitcoin reprezintă încercarea de a introduce o monedă digitală care a înregistrat cel mai mare succes din ultimii zece ani, așa spune eu.

JULIAN: Aproape că au descoperit echilibrul perfect. Eu cred că Bitcoin va continua. Este o monedă eficientă; poți să-ți deschizi un cont în zece secunde, iar pentru a transfera bani de acolo nu suporti alte cheltuieli decât costul unei conexiuni la internet și a câtorva minute de electricitate. Este foarte competitiv în comparație cu oricare altă modalitate de transfer monetar. Cred că va prospera. Uitați-vă doar la ce s-a întâmplat în urma unor furturi de Bitcoin și a unor recenzii negative în presă, în vara lui 2011, care au coborât rata de schimb la trei dolari SUA.⁹⁴ Bitcoin s-a ridicat treptat înapoi la doisprezece dolari. Nu a crescut brusc, nu și-a revenit dintr-un singur salt, ci s-a ridicat într-un mod gradual care pare să indice o cerere crescândă pentru această monedă. Suspectez că o mare parte din această cerere se datorează micului trafic de droguri, comenzilor de marijuana prin poștă și așa mai departe.⁹⁵ Dar Bitcoin are cheltuieli mici ca monedă. Mai multe ISP-uri încep să o folosească, mai cu seamă în țări în care nu ai

acces ușor la servicii de card de credit, cum ar fi fosta Uniune Sovietică.

Vor exista măsuri împotriva ei dacă va continua să crească. Nu vor putea să elimine moneda Bitcoin, din cauză că procedeele criptografice împiedică reușita oricărui atac coercitiv, dar genul de servicii de schimb valutar care schimbă în și din Bitcoin vor putea fi împiedicate mult mai ușor să funcționeze. Pe de altă parte, aceste schimburi valutare pot funcționa oriunde în lume, deci sunt destule jurisdicții prin care trebuie să treci ca să nu mai existe servicii de schimb valutar și, de asemenea, piața neagră are propria sa logică în materie de schimb valutar. Eu cred că modul în care trebuie abordată moneda Bitcoin este să se încerce ca ea să fie adoptată de ISP-uri și de industria serviciilor de internet pentru genul de jocuri mici, pe care le cumperi pe Facebook și așa mai departe, din cauză că este atât de eficientă, și, odată ce a fost adoptată de mai multe industrii, ele vor forma un lobby pentru a împiedica interzicerea ei. Este, într-un fel, modul în care a fost adoptată criptografia. La început a fost inclusă în aceeași categorie cu comerțul de arme, iar unii dintre noi au fost numiți comercianți de arme, dar odată ce a fost în browsere și a fost folosită pentru servicii bancare, s-a creat un lobby destul de puternic pentru a-i împiedica interzicerea – deși mă văd nevoit să recunosc că sunt din nou în pregătire mișcări în acest sens.

JACOB: Problema este că îngrijorările legate de confidențialitate sunt false. Hai să fim cinstiți. Este fals să sugerezi că aspectele economice ale situației de față sunt altfel cu internet decât fără internet. Când am ajuns aici și am cumpărat lire sterline a trebuit să predau CNP-ul, care este identificatorul meu unic în Statele Unite, a trebuit să-mi predau numele, a trebuit să conectez numele și contul bancar, a trebuit să le dau banii. Au înregistrat toate numerele de serie și apoi au luat toate acele informații și le-au

transmis guvernului federal. Deci aceasta e analogia. De fapt, este mai greu să cumperi valută străină în SUA, din cauză că suntem atât de îndepărtați de toate celelalte țări. Dar există o tendință istorică în ceea ce privește controlul monedei și nu vedem acest control doar în legătură cu internetul. Mai mult decât atât, am înțeles că există bancomate în unele bănci care înregistrează numerele de serie ale bancnotelor, iar apoi le urmăresc, pentru a face analize de flux al bancnotelor, pentru a vedea unde au fost cheltuite și cine ce a făcut cu ele.

Dacă ne uităm la aceste sisteme, iar apoi ne întoarcem privirea la internet, nu au îmbunătățit confidențialitatea, pe măsură ce am migrat către internet – de fapt, au păstrat-o la fel de proastă cum era înainte. În acest sens, cred că este foarte important să ne uităm la tendințele din lumea de dinaintea internetului pentru a vedea încotro ne îndreptăm. Ceea ce observăm este că dacă ai mulți bani poți plăti o taxă pentru a-ți păstra confidențialitatea, iar dacă nu ai mulți bani, e aproape garantat că nu ai confidențialitate. Și este și mai rău în cazul internetului. Lucrurile ca Bitcoin sunt un pas în direcția corectă, fiindcă atunci când este combinat cu un canal anonim de comunicații, cum ar fi Tor, de pildă, îți permite să trimiți un Bitcoin către WikiLeaks prin intermediul sistemului Tor, și oricine ar privi această tranzacție ar vedea un utilizator Tor trimițând un Bitcoin, iar pe tine primindu-l. Este posibil lucrul acesta – în unele privințe este mult mai bun decât moneda clasică.

JULIAN: Cu toții vorbim despre confidențialitatea comunicațiilor și dreptul de a publica. Acestea sunt lucruri destul de lesne de înțeles – au o istorie lungă în spatele lor – și, în realitate, jurnaliștii adoră să vorbească despre ele pentru că-și protejează propriile interese. Dar dacă am compara valoarea lor cu valoarea confidențialității și libertății interacțiunilor economice, de fapt, de fiecare dată când CIA urmărește o interacțiune economică, ei

pot vedea că este din partea cutarei persoane, din cutare loc, către cutare persoană în cutare loc și pot să estimeze astfel valoarea și importanța interacțiunii. Deci nu este cumva libertatea sau confidențialitatea interacțiunilor economice mai importantă decât libertatea de exprimare, din cauză că interacțiunile economice se află la baza întregii structuri a societății?

JACOB: Ele sunt legate intrinsec. Cred că aici se poate observa diferența dintre activiștii cypherpunk americani și cei europeni, din cauză că majoritatea activiștilor americani ar spune că ele sunt același lucru. Fiindcă într-o societate cu o economie de piață liberă, ai putea spune că-ți demonstrezi vorbele prin fapte.

JULIAN: Dar o faci urmărind în același timp să-ți consolidezi puterea.

JACOB: Exact. Nu vreau să spun că e corect așa, e aproape o atitudine de dreapta față de chestiunea asta, care poate nu este ceea ce vrem noi. Poate vrem un capitalism social, de exemplu.

JULIAN: Dacă ar fi să ne uităm doar dintr-o perspectivă de spionaj: ai un buget de 10 milioane de dolari. Poți spiona interacțiunile pe e-mail ale oamenilor sau le poți supraveghea toate interacțiunile economice. Ce preferi?

ANDY: Păi, în zilele noastre ar spune: „Bine, vom obliga companiile de plăți și băncile să folosească internetul, și astfel împușcăm amândoi iepurii“. Și asta este chiar ceea ce au făcut. Deci concluzia este că nu mai există o scăpare directă. Poți să folosești Tor, de exemplu, pentru a-ți proteja comunicațiile, poți să-ți criptezi convorbirile telefonice, poți să-ți securizezi mesageria. În privința banilor, lucrurile sunt mult mai complicate și există de pildă legi împotriva spălării de bani și așa mai departe, și ni se

spune că organizațiile teroriste și de trafic de droguri abuzează de infrastructură pentru a face rău.

JACOB: Sunt Călăreții Apocalipsei Informatice.

ANDY: De fapt, aș fi foarte interesat să avem mai multă transparență în privința cheltuielilor efectuate de companiile de supraveghere și de guverne pentru aceste chestiuni. Întrebarea este ce avem de câștigat dacă acordăm anonimitate totală doar sistemului monetar? Ce s-ar întâmpla în realitate? Eu cred că lucrul acesta ar putea conduce ici și colo la fenomene interesante în care oamenii ar putea să-și ușureze puțin situația și să spună: „Păi, știi, aș putea să-mi ridic vocea, aș putea să merg în Parlament, dar aș putea la fel de bine să mituiesc niște politicieni“.

JÉRÉMIE: Descrii situația din SUA, nu-i așa?

JACOB: Nu e anonim.

ANDY: Nu sunt atât de sigur că situația e doar a SUA. În Germania nu-i spunem corupție, spunem că sunt fundații care cumpără tablouri ale soțiilor politicienilor, așa că vorbim de comerțul de artă și de diverse alte domenii. Deci avem denumiri mai bune. S-ar putea ca în Franța să i se spună petreceri ale prieteniei, iar alții să-i spună angajare de prostituate.

JÉRÉMIE: În SUA este un caz special, din cauză că legătura dintre sistemul politic și bani e foarte strânsă. După ce a lucrat zece ani în domeniul drepturilor de autor, Larry Lessig a spus că a renunțat să mai încerce să remedieze problema drepturilor de autor (de fapt, nu a renunțat), din cauză că și-a dat seama că problema n-o reprezenta opinia politicienilor despre ce înseamnă o politică bună de copyright, problema era că există pur și simplu prea multe legături cu actorii industriali care încearcă să instaureze un regim

prost al drepturilor de autor.⁹⁶ Deci avem aici o problemă cât se poate de reală.

JULIAN: Ești sigur că este o problemă, Jérémie? Poate că de fapt este o însușire bună aceea că industriile care sunt productive...

ANDY: Cred că avocatul diavolului îmi bea din whisky.

JACOB: Hai să vedem dacă poate termina propoziția asta fără să izbucnească în râs. Provoacă-ne, Maestre Provocator.

JULIAN: Acele industrii care sunt productive, care produc bogăție pentru întreaga societate folosesc o parte din banii lor pentru a se asigura că rămân productive, înlăturând legislațiile aiurea care se nasc dintr-o mitologizare politică, rezultat al exagerărilor. Iar cea mai bună modalitate de a face asta chiar este să mituiești membri ai Congresului, să folosești activitatea industriei productive pentru a modifica legea – astfel încât să menții productivitatea industriei.

JACOB: Stați – am să răspund eu la asta. Sunteți gata? Sunteți gata? Acum, sunteți gata? Nu.

JULIAN: De ce?

JACOB: Sunt mai multe motive, dar, în primul rând, există o buclă de reacție extrem de negativă. De exemplu, cred că unul dintre cei mai mari sponsori de campanie din statul California este sindicatul paznicilor de închisoare, și asta pentru că vor să facă lobby pentru legi mai dure – nu fiindcă ar fi interesați de domnia legii, ci fiindcă așa ceva ar fi în avantajul meseriei lor.⁹⁷ Deci dacă vezi că oamenii aceștia fac lobby pentru construirea mai multor închisori, pentru închiderea mai multor oameni, pentru prelungirea duratei sentințelor, ce fac ei în realitate? Ceea ce fac ei este să se folosească de câștigurile pe care le au de pe urma activității

lor benefice – indiscutabil – pentru a extinde monopolul pe care li-l acordă statul.

JULIAN: Deci se folosesc de asta pentru a transfera banii de la industriile productive la cele care nu produc nimic?

JACOB: Ai putea să spui și așa.

JULIAN: Dar poate că asta este doar o componentă minoră. De orice sistem se abuzează, poate că acești profitori care se ocupă doar cu transferurile de bani reprezintă un element minor și, de fapt, cea mai mare parte a lobby-ului, cea mai mare influență asupra Congresului vine din partea industriilor productive, care se asigură că legile vor continua să permită acestor industrii să fie productive.

JACOB: Dar poți măsura lucrul ăsta foarte ușor, fiindcă poți căuta care sunt oamenii care doresc să promoveze activități de tipul *rent-seeking* și care vor să restricționeze libertatea altor oameni pentru a crea o situație în care ei înșiși nu ar fi putut să se ridice la nivelul la care sunt astăzi. Când fac lucruri de genul acesta știi că ceva nu este în regulă și că pur și simplu încearcă să apere lucrurile pe care le au, lucruri pe care le-au agonisit, în principal, printr-o exploatare – de regulă, printr-un apel la emoții prin care spun: „Vai, opriți teroristul, opriți pornografia infantilă, opriți spălarea de bani, declarați război drogurilor“. Se poate ca aceste lucruri să fie cât se poate de rezonabile în contextul în care au fost prezentate inițial, și de regulă chiar sunt, fiindcă, în general vorbind, credem că aceste lucruri sunt rele pentru că există un element grav în fiecare dintre ele.

ANDY: Aș vrea să mă întorc la chestiunea drepturilor de autor și să vă mai dau un exemplu – au existat probleme serioase când au apărut automobilele. Cei care conduceau companii de transport

al pasagerilor cu ajutorul cailor se temeau că asta avea să le ucidă afacerea, lucru care s-a întâmplat, dar poate că avea și o logică. Am fost invitat să vorbesc la asociația companiilor de film din Germania, iar înaintea discursului meu a fost un profesor al unei universități din Berlin care a vorbit foarte politicos despre evoluția rasei umane și dezvoltarea culturii, spunând că copierea gândurilor și procesarea lor ulterioară sunt elementul-cheie, tot așa cum regia de film ține de preluarea unor teme și exprimarea lor într-o manieră dramaturgică. După cele patruzeci de minute pe care le avea la dispoziție, moderatorul l-a întrerupt cu neobrăzare și a spus: „Ok, după ce tocmai ați spus că trebuie să legalizăm furtul, haideți să vedem ce are să ne spună tipul de la Chaos Computer Club“. Și m-am gândit: „Wow, ce căcat? Dacă e să-mi spun răspicat părerea, o să mai ies întreg de aici?“ Deci unele industrii au pur și simplu pledoarii care nu slujesc evoluției. E un mod egoist de a proceda, faptul că se blochează în abordarea lor antievoluționistă care face ca totul să fie și mai monopolizat. Și când au apărut casetele au crezut că industria muzicală va dispărea. S-a întâmplat opusul, industria a explodat. Întrebarea e care e politica aici? Care este modalitatea pozitivă în care ai putea formula aceste lucruri?

JULIAN: Mă întreb dacă nu am putea, de fapt, să standardizăm practica actuală din Statele Unite și să o legiferăm astfel încât pur și simplu să mituiești senatori și să cumperi voturi în Senat.

JÉRÉMIE: Nu, nu, nu, nu.

ANDY: Hai să presupunem că avem banii necesari.

JULIAN: Da, și că totul este pe față și că există cumpărători și că fiecare merge la o licitație.

ANDY: Dar industria de armament ar avea oricum mai mulți bani.

JULIAN: Nu, cred că nu ar avea. Cred, de fapt, că complexul militar-industrial ar fi relativ marginalizat, deoarece capacitatea lor de a funcționa în spatele ușilor închise, într-un sistem care nu este deschis procesului de licitații de piață, este mai mare decât a altor industrii.

JACOB: Există o inegalitate fundamentală în sistem.

JÉRÉMIE: Dintr-o perspectivă economică liberală, antimonopol, când spui hai să lăsăm actorii dominanți să decidă care va fi politica, îți pot răspunde pe baza experienței internetului ultimilor cincisprezece ani, unde inovația se producea prin așa-numitul sistem de jos în sus, unde practici noi apăreau de nicăieri, unde doi tipi inventau o tehnologie de succes într-un garaj.

JULIAN: Aproape totul, Apple, Google, YouTube, totul.

JÉRÉMIE: Totul. Tot ceea ce a apărut pe internet a explodat pur și simplu după ce cu câteva luni sau câțiva ani înainte fusese necunoscut, deci nu poți să prezici care ar putea fi următoarea inovație, iar ritmul inovațiilor este atât de rapid, încât este mult mai rapid decât procesul de elaborare de politici. Deci când elaborezi o lege care să aibă un impact asupra pieței așa cum e ea astăzi, asupra relațiilor de putere dintre diferitele companii și actori economici așa cum se prezintă ei astăzi, dacă acorzi mai multă putere cuiva care este deja puternic, poți bloca apariția unui nou actor care ar fi fost mai eficient.

JULIAN: Piața trebuie să fie reglementată pentru a fi liberă.

JÉRÉMIE: Firește că trebuie să lupți împotriva monopolurilor și că ai nevoie de o putere care să fie superioară puterii companiilor în cauză pentru a putea pedepsi comportamentele neregulate – dar ceea ce vreau să spun aici este că politicile trebuie să

se adapteze la societate, nu invers. În cazul războaielor copyright avem impresia că legislatorul încearcă să schimbe întreaga societate pentru a se adapta la un șablon definit de Hollywood, de exemplu. „Uitați care e treaba, ceea ce faceți acum, cu noile practici culturale, este pur și simplu greșit din punct de vedere moral, iar dacă nu vreți să încetați, vom elabora instrumente legale care să vă facă să încetați a mai face ceea ce credeți voi că e bine.” Nu așa se elaborează o politică bună. O politică bună privește lumea și încearcă să se adapteze, astfel încât să corecteze ceea ce este greșit și să permită în continuare ceea ce este bine. Sunt convins că atunci când le permiți celor mai puternici actori economici să decidă în privința politicilor, nu urmezi calea asta.

ANDY: Eu încerc pur și simplu să vă stimulez să vă gândiți – și eu împreună cu voi – care ar fi o politică bună. Ceea ce ai formulat tu mi se pare, în momentul de față, puțin prea complicat. Încerc să simplific puțin lucrurile. Există un tip pe care-l cheamă Heinz von Foerster – nașul ciberneticii – care a elaborat la un moment dat un set de reguli, iar una dintre aceste reguli era „Acționează tot timpul în așa fel încât să sporești opțiunile”.⁹⁸ Așadar, în cazul politicilor, al tehnologiei, a orice, fă tot timpul ceea ce-ți aduce mai multe, nu mai puține opțiuni.

JULIAN: Și în cazul strategiei de șah e la fel.

ANDY: S-a spus că amplificarea confidențialității tranzacțiilor monetare ar putea avea un efect negativ, așa că trebuie să ne gândim: „În momentul de față, sistemul monetar are o logică specifică și chestiunea importantă este cum împiedicăm sistemul monetar să invadeze alte arii de activitate”. Fiindcă sistemul monetar are posibilitatea – spre deosebire de sectorul de comunicații – să afecteze și să limiteze opțiunile pe care le au oamenii în alte arii de activitate. Dacă poți plăti asasini pentru a face anumite lucruri, sau

dacă îți poți cumpăra arme și merge la război împotriva altor țări, atunci limitezi opțiunile altor oameni de a trăi, de a acționa. Dacă investesc mai mulți bani în comunicații, atunci mai mulți oameni ar avea mai multe opțiuni. Dacă aduc pe piață mai multe arme...

JACOB: Nu – cu cât ai o mai mare posibilitate de a supraveghea, cu atât ai mai mult control.

ANDY: Ceea ce reprezintă încă un argument bun pentru a restricționa piața de armament, inclusiv tehnologia de supraveghere a telecomunicațiilor.

JACOB: Da, sigur, vrei să-mi restricționezi capacitatea de a vinde lucrurile acestea, dar cum o vei face? Cum îmi poți restricționa capacitatea de a transfera bogății? – tot prin rețelele de comunicații. În Statele Unite, unul dintre cele mai ofensatoare aspecte legate de sprijinele financiare* acordate – ofensatoare pentru mulți oameni, dintr-o mulțime de motive – a fost faptul că au arătat că banii nu sunt nimic mai mult decât o serie de biți într-un sistem informatic. Unii oameni, cerșind într-un mod foarte eficient, au reușit să determine creșterea valorii multora dintre acești biți, și atunci care e întrebarea? Are vreo valoare sistemul dacă poți trișa pur și simplu și crește valoarea biților tăi? Iar tuturor celorlalți care să străduiesc să se descurce nu le este recunoscut faptul că au și ei biți care merită să fie măcar luați în considerare.⁹⁹

ANDY: Deci ceea ce vrei tu să spui este că avem nevoie de un sistem economic complet diferit? Pentru că în ziua de astăzi valoarea nu este legată de valoarea economică.

JACOB: Nu, spun că există o valoare economică.

* Este vorba despre așa-numitele „bailouts”, sprijine financiare acordate de guvernul SUA unor companii sau țări aflate în dificultate financiară sau în faliment. (n.tr.)

ANDY: Poți face bani din ticăloșii, și poți produce lucruri bune fără să iei un sfanț pe ele.

JACOB: Păi nu, ceea ce vreau să spun este că nu poți să decuplezi economia de comunicații. Nu spun că avem sau nu nevoie de un alt sistem economic. Nu sunt economist. Voi spune doar că sistemele de comunicații și libertatea acelor comunicații au o oarecare valoare, la fel cum libertatea schimbului în natură are o valoare – am dreptul să-ți dau ceva în schimbul muncii tale, la fel cum am dreptul să-ți explic o idee, iar tu ai dreptul să-mi spui ce crezi despre ideea mea. Nu putem spune că sistemul economic se află într-un soi de vid. Sistemul de comunicații este legat de el în mod direct, iar lucrul ăsta face parte din societate.

Dacă e să avem această noțiune reduționistă despre libertate, despre cele trei libertăți pe care le-a menționat Julian, aceasta este legată în mod evident de libertatea de mișcare – astăzi nu poți nici măcar să-ți cumperi un bilet de avion fără să folosești o monedă care poate fi urmărită, fiindcă în caz contrar vei fi însemnat cu un steguleț. Dacă intri într-un aeroport și încerci să-ți cumperi un bilet în aceeași zi cu bani în numerar, vei fi însemnat. Vei fi supus unor proceduri de verificare suplimentare, nu vei putea zbura fără a te fi legitimat, iar dacă ai avut ghinionul să-ți cumperi biletul de avion cu cardul de credit, vor înregistra totul despre tine – de la adresa ta de IP până la browserul folosit. Eu chiar am datele mele, obținute conform Legii libertății informației, din arhiva Serviciului pentru Controlul Imigrației și Normelor Vamale de acum câțiva ani, pentru că m-am gândit că va fi interesant să mă uit la diferențe într-o bună zi. Și, ca să vezi, e inclus acolo și Roger Dingledine, care mi-a cumpărat un bilet de avion pentru o chestie legată de muncă, e inclus cardul său de credit, adresa locului în care se afla când l-a cumpărat, browserul pe care l-a folosit și toate informațiile despre biletul de avion, toate înregistrate împreună.

JULIAN: Și toate acestea au mers către guvernul SUA, nu au fost doar stocate în procesorul comercial?

JACOB: Exact. Datele comerciale au fost colectate, trimise către guvern și au fost stocate împreună. Iar lucrul care mi s-a părut complet nebunesc este că, în esență, este vorba despre fuzionarea acestor trei lucruri de care vorbești tu. Era dreptul meu să călătoresc liber, era capacitatea mea să cumpăr acel bilet de avion sau ca altcineva să-l cumpere, și era vorba, efectiv, de capacitatea mea de a mă exprima – călătoream pentru a ține un discurs undeva, iar pentru a face acel lucru a trebuit să fac compromisuri în celelalte două sfere. Și de fapt îmi lezează capacitatea de a mă exprima, mai cu seamă când aflu mai târziu ce au colectat și faptul că au stocat totul la un loc.

Cenzura

JULIAN: Jake, poți să spui câte ceva despre faptul că ai fost reținut în aeroporturile SUA și despre motivul pentru care s-a întâmplat?

JACOB: Mi-au spus că se întâmplă din cauză că „știu eu de ce“.

JULIAN: Dar n-au spus de ce?

ANDY: Pot să încerc eu să rezum chestiunea, fiindcă securitatea tehnică și securitatea afacerilor guvernamentale sunt două lucruri complet distincte. Poți avea un sistem tehnic cât se poate de securizat și guvernul va crede că nu este bun de nimic, pentru că ei cred că securitatea este atunci când pot observa ce se întâmplă în interiorul său, când îl pot controla, când pot sparge securitatea tehnică. Ceea ce s-a întâmplat nu s-a întâmplat din cauză că Jake ar fi încercat să se apropie de vreun avion, să omoare pe cineva, să deturneze un avion sau mai știu eu ce. A fost vorba despre capacitatea sa de a afecta afacerile guvernamentale călătorind în alte țări, comunicând cu oamenii, răspândind idei. Acesta este cel mai periculos lucru care se poate întâmpla unui guvern în ziua de astăzi – când ideile oamenilor sunt mai bune decât politica lor.

JACOB: Apreciez foarte mult complimentul pe care mi l-ai făcut prin afirmația asta, dar aș vrea să subliniez că ceea ce s-a întâmplat

este mult mai rău decât atât, pentru că de la toată lumea se colectează genul acesta de date. Aceasta s-a întâmplat înainte să fi făcut eu ceva interesant; era vorba despre simplul fapt că plecam într-o călătorie, iar sistemele însele, arhitectura, promovau colectarea aceasta de informații. Aceasta s-a întâmplat înainte să fi fost oprit pentru ceva, înainte să fi fost deportat din Liban, înainte ca guvernul SUA să fi avut vreun interes special față de mine.

ANDY: Poate au prevăzut ceva, poate au observat ceva înainte să o fi făcut tu.

JACOB: Binențeles, în parte din cauza colectării acestor date. Dar de fiecare dată îmi dau un alt răspuns. De obicei au un singur răspuns: „Pentru că putem“. Și eu le spun: „Bine, nu vă pun la îndoială autoritatea – de fapt, ba da, vă pun la îndoială autoritatea, doar că nu o fac acum –, vreau pur și simplu să știu de ce mi se întâmplă lucrurile astea“. Acum mi se spune tot timpul: „Păi nu e evident? Lucrezi la Tor“ sau „Stai pe scaunul de lângă Julian, la ce te așteptai?“ Mi se pare fascinant că fiecare dintre cei care mă rețin – de regulă de la Serviciul Vamal și de Protecție a Frontierei sau de la Serviciul pentru Controlul Imigrației și Normelor Vamale din Statele Unite – îmi spune că, mai mult decât orice, o fac din cauză că au autoritatea să o facă. Mi s-au spus și rahaturi de genul „Îți amintești de 11 septembrie? De aia“, sau „Pentru că vrem să ne răspunzi la niște întrebări, iar asta este locul în care ai cele mai puține drepturi, sau cel puțin așa spunem noi“.

Iar în situații de genul acesta îți vor refuza accesul la un avocat, îți vor refuza accesul la o toaletă, dar îți vor da apă, îți vor da ceva de băut, un diuretic, de exemplu, pentru a te convinge că e în interesul tău să cooperezi în vreun fel. Au făcut acestea pentru a mă presa, din motive politice. Mi-au pus întrebări despre părerea mea în legătură cu războiul din Irak, despre părerea mea

în legătură cu războiul din Afganistan. Practic, au repetat tacticile folosite de FBI în timpul operațiunii COINTELPRO (uriașul program de operațiuni domestice sub acoperire care a fost în funcțiune între 1956 și 1971). De pildă, au încercat în mod direct să-și afirme autoritatea de a schimba realități de ordin politic din viața mea și de a încerca să mă preseze nu doar să le schimb, ci să le acord un soi de cale specială de acces la ceea ce se petrece în capul meu. Și mi-au confiscat lucruri aflate în proprietate. Nu prea sunt autorizat să vorbesc despre toate lucrurile care mi s-au întâmplat pentru că este o zonă gri și foarte obscură și nici nu știu exact dacă mi-e permis măcar să vorbesc în general despre ele. Sunt sigur că s-au întâmplat și altor oameni, doar că eu nu am auzit niciodată să li se fi întâmplat.

Eram odată la aeroportul Pearson din Toronto, mă întorceam acasă de la o întâlnire cu familia. Călătoream spre Seattle, unde locuiam în acea vreme, și m-au reținut, m-au dus la un control de securitate secundar, apoi la un control de securitate terțiar, iar într-un final într-o celulă de detenție. Și m-au ținut acolo atât de mult, încât când într-un final mi-au dat drumul, am ratat zborul. Dar lucrul curios este că aceste zone de predetenție sunt de fapt teritoriu american pe teritoriul canadian, așa că au o regulă conform căreia, dacă ți-ai ratat zborul sau dacă mai e foarte mult până la următorul zbor, ești obligat să pleci. Deci am fost de fapt dat afară din America din cauză că am fost reținut atât de mult și a trebuit să intru în Canada, să zbor în altă parte a țării, să-mi închiriez o mașină, apoi să trec frontiera cu mașina. Și când am ajuns la frontieră mi-au spus: „Cât timp ați petrecut în Canada?“, iar eu le-am spus „Păi, cinci ore plus reținerea din Toronto“, deci fusesem în Canada vreo opt ore, și mi-au spus „Intrați, și vă vom reține din nou“. Apoi mi-au făcut mașina bucăți, mi-au dezmembrat laptopul, s-au uitat prin toate aceste lucruri, după care m-au reținut. Mi-au permis accesul la o toaletă după o jumătate

de oră, s-ar putea spune că au fost foarte milostivi. Iar asta este ceea ce ei numesc percheziția vamală de excepție – genul acesta de comportament are loc pentru că au capacitatea, spun ei, să o facă, și nimeni nu le poate imputa nimic în legătură cu asta.¹⁰⁰

JULIAN: Așadar, acestea ți s-au întâmplat ție, dar persoanele din China cu care vorbesc, când îmi spun despre marele firewall al Chinei – în Occident vorbim în principal despre asta în termeni de cenzură, despre faptul că cetățenii Chinei sunt împiedicați să iasă și să citească ce se spune despre guvernul chinez în Occident, de către disidenți chinezi, de către Falun Gong și de către BBC și, s-o recunoaștem, în însăși propaganda despre China –, dar îngrijorarea lor nu este de fapt legată de cenzură. Ceea ce-i îngrijorează este că pentru cenzurarea internetului e nevoie și de supravegherea sa. Pentru a verifica ce pagini accesează cineva, pentru a vedea dacă acestea sunt permise sau restricționate, trebuie să le poți vedea, iar dacă le vezi înseamnă că le poți și arhiva. Iar lucrul acesta a avut efectul de a înspăimânta populația Chinei – nu faptul că sunt supuși cenzurii, ci faptul că tot ceea ce citesc este spionat și înregistrat. În realitate, lucrul acesta este adevărat și pentru noi. Acesta e un lucru care schimbă oamenii, în momentul când îl conștientizează. Le modifică comportamentul, iar ei devin mai puțin fermi în nemulțumirea față de diferite autorități.

JACOB: Aceasta este totuși o reacție greșită la genul acela de influență. Hărțuirea pe care am suferit-o la frontiere, de exemplu, nu e unică, în sensul că, după și chiar înainte de 11 septembrie, fiecare cetățean american de origine arabă a trebuit să treacă prin așa ceva. Doar că eu refuz să-mi irosesc privilegiul de a avea pielea albă și pașaport SUA și refuz să tac în legătură cu asta, pentru că lucrurile pe care le fac aceste persoane nu sunt corecte și pentru că abuzează de puterea pe care o folosesc. Și trebuie să ne opunem

acestor lucruri, la fel cum există și în China persoane curajoase care se opun, cum ar fi Isaac Mao, de pildă.¹⁰¹ El s-a opus foarte vehement, și în mod eficient, acestui gen de cenzură, pentru că reacția adecvată nu este pur și simplu să cedezi în fața acestui tip de presiune doar din cauză că guvernul afirmă că are puterea să o facă.

JÉRÉMIE: Dar aici vorbim din nou despre politică, pentru că ceea ce spui tu este, în esență, că oamenii ar trebui să lupte pentru drepturile lor – dar oamenii ar trebui să înțeleagă de ce trebuie să o facă, iar apoi ar trebui să aibă capacitatea de a comunica unii cu alții pentru a o face. Am avut ocazia să vorbesc cu unele persoane din China – și nu știu dacă ocupau vreo poziție în stat sau dacă au fost selectate pentru a putea să iasă și să vorbească cu mine –, dar când i-am întrebat despre cenzura internetului, am primit foarte des acest răspuns: „Păi, este pentru binele Poporului. Există cenzură, sigur, pentru că dacă nu ar fi existat cenzură ar fi existat comportamente extremiste, ar fi existat lucruri neplăcute pentru toată lumea, iar guvernul ia aceste măsuri pentru a se asigura că totul merge bine“.

JACOB: Este același argument precum cel pentru prelevarea de organe. Nu faceți risipă de organe!

JÉRÉMIE: Dacă ar fi să ne uităm la modul în care este implementată cenzura în China, am vedea că, din punct de vedere tehnic, este unul dintre cele mai avansate sisteme din lume.

JACOB: Foarte adevărat.

JÉRÉMIE: Și am auzit că pe Weibo – care este echivalentul chinezesc al Twitter-ului – guvernul poate filtra unele *hashtags* pentru a se asigura că ele nu părăsesc o anumită provincie.

JACOB: Este esențial să nu pierdem din vedere faptul că atunci când se vorbește despre cenzura din Asia, ne place să vorbim în termeni de „celălalt” – de parcă afectează doar oamenii din „X-istan”. Este foarte important să se știe că atunci când cauți pe Google în Statele Unite, îți spun că au omis unele rezultate din considerente legale. Există o diferență între cele două – atât la nivelul modului în care sunt implementate, cât și, evident, la nivel de realitate socială a lui cum, al lui de ce, chiar și a lui unde privitor la cenzură – dar o mare parte a diferenței ține de arhitectură. De exemplu, asupra internetului american, fiind foarte descentralizat, este foarte greu să implementezi o cenzură după modelul Chinei.

JULIAN: Ei bine, o mare parte a sa e reprezentată de Google, iar Google poate fi cenzurat. Există o grămadă de pagini care fac referire la WikiLeaks și care sunt cenzurate de Google.

JACOB: Da, fără îndoială. Și, de fapt, pentru că indexul ca atare este liber, se poate face o analiză diferențială.

JULIAN: Da, teoretic.

JACOB: Teoretic. Iar practic, există niște persoane care lucrează la genul acesta de detector de cenzură uitându-se la diferențele văzute din diferite perspective din lume. Cred că este important să ne amintim că cenzura și supravegherea nu sunt probleme din „alte locuri” – occidentalilor le place să vorbească despre cum „oamenii din Iran, China și Coreea de Nord au nevoie de anonimitate și libertate, dar aici nu avem nevoie de ele”. Și când spun „aici” vor de regulă să spună „în Statele Unite”. Dar de fapt nu e vorba doar de regimuri politice opresive, fiindcă dacă se întâmplă să faci parte din eșalonul de top al oricărui regim, pentru tine nu va fi opresiv. Dar avem impresia că Regatul Unit este

un loc minunat; de regulă se crede că Suedia ar fi o țară splendidă, și totuși putem vedea că atunci când ieși din grațiile celor aflați la putere, nu ajungi într-o poziție favorabilă. Dar Julian este încă în viață, nu-i așa? Deci e clar că acesta este un semn că avem de-a face cu o țară liberă – am dreptate?

JULIAN: Am muncit mult pentru a-mi menține poziția pe care o am acum. Dar poate că ar trebui să vorbim despre cenzura internetului în Occident. Este un lucru foarte interesant. Dacă ne întoarcem în anul 1953 și ne uităm la marea Enciclopedie sovietică, care a fost distribuită peste tot, vedem că ea a suferit modificări de fiecare dată când au existat schimbări de ordin politic în Uniunea Sovietică. În anul 1953 a murit Beria, șeful NKVD-ului, poliția secretă sovietică, și a ieșit din favorurile politice, astfel că secțiunea sa, care-l descria în termeni strălucitori, a fost tăiată de către autoritățile care se ocupau de enciclopedie, care au emis un amendament ce trebuia introdus în toate aceste enciclopedii. Era extrem de evident. Menționez acest exemplu din cauză că era atât de evident și putea fi detectat atât de ușor încât încercarea aceasta a devenit istorică. În timp ce în Regatul Unit avem *The Guardian* și alte ziare importante care scot în secret articole din arhivele lor online fără nici un fel de explicații. Dacă ați accesa paginile acestea acum și ați încerca să le găsiți, de exemplu articole despre cazul de fraudă al miliardarului Nadhmi Auchi, ați primi rezultatul „Page Not Found“, și au fost scoase și din indexuri.

Să vă povestesc despre implicarea mea în povestea lui Nadhmi Auchi. În anul 1990, Irakul a invadat Kuwaitul, iar asta a dus la primul Război din Golf. Guvernul Kuwaitului a avut nevoie de bani în timpul exilului, dar și după reîntoarcerea în țară, așa că a început să scoată la vânzare mai multe bunuri, inclusiv câteva rafinării de petrol din afara granițelor țării. Un afacerist englez,

Nadhmi Auchi, care imigrase în anii '80 în Regatul Unit din Irak, unde fusese un personaj în regimul lui Saddam Hussein, a fost broker în acea vânzare și a fost după aceea acuzat că ar fi fost implicat în transferul de comisioane ilegale în valoare de 118 milioane de dolari. Acea investigație a fost cea mai mare investigație de corupție din istoria Europei de după război. În anul 2003, Nadhmi Auchi a fost declarat vinovat de fraudă în ceea ce a devenit cunoscut ca Scandalul Elf Aquitaine. Cu toate acestea, astăzi are peste 200 de companii înregistrate în holdingul său din Luxemburg și altele în Panama. Este implicat într-o afacere de telefonie mobilă în Irak și în multe alte afaceri pe glob.¹⁰²

În Statele Unite, Tony Rezko, care a strâns fonduri pentru campania pentru Senat a lui Barack Obama, era un amic vechi de-al lui Auchi, acesta din urmă fiind în trecut finanțatorul său. De asemenea, Auchi și Rezko s-au asociat cu fostul guvernator al statului Illinois, Rob Blagojevich. Atât Rezko, cât și Blagojevich au fost găsiți vinovați de corupție, Rezko în 2008, iar Blagojevich în 2010/2011 (după ce FBI-ul i-a înregistrat un apel telefonic interceptat în care încerca să vândă fostul loc în Senat al lui Obama). În 2007/2008, când Obama era în campania pentru a fi ales candidatul partidului Democrat la alegerile prezidențiale, presa din SUA a început să investigheze relațiile lui Obama. L-au investigat pe Rezko și au găsit niște conexiuni relativ la cumpărarea casei lui Barack Obama. În 2008, cu puțin timp înaintea procesului său, Rezko a primit prin transfer 3,5 milioane de dolari de la Auchi pe care nu i-a declarat Curții, deși era obligat să o facă – motiv pentru care a și fost închis. Așa că cercetările amănunțite ale presei din SUA s-au îndreptat către Auchi, iar în acel moment el a poruncit avocaților de la Carter-Ruck din Regatul Unit să înceapă o campanie agresivă împotriva unei mari părți a reportajelor din 2003 despre scandalul Elf Aquitaine și condamnarea sa în Franța. Campania a avut un mare succes.

S-a îndreptat împotriva presei din Regatul Unit, dar și împotriva unor bloguri din SUA și a cerut scoaterea de pe internet a cel puțin 12 articole, din câte știm noi. Majoritatea acelor articole, inclusiv cele din arhivele ziarelor din Regatul Unit, au dispărut, pur și simplu. Era ca și cum nici nu ar fi existat vreodată. Nu a existat nici un soi de „Am primit o plângere de ordin juridic și am decis să scoatem articolul“. Au dispărut și din indexuri. WikiLeaks le-a scos la iveală și le-a publicat din nou.¹⁰³

JACOB: Ei șterg istoria.

JULIAN: Istoria nu e doar modificată, ci a încetat să fi existat vreodată. Este dictonul lui Orwell: „Cel care controlează prezentul controlează trecutul, iar cel care controlează trecutul controlează viitorul.“ Este ștergerea imposibil de detectat a istoriei în Occident, iar asta este doar cenzura de după publicare. Autocenzura dinaintea publicării este mult mai gravă, dar deseori greu de detectat. Am putut observa asta în cazul publicării Cablegate, pentru că WikiLeaks lucrează cu mai mulți parteneri media pe tot mapamondul, deci putem vedea care dintre ei cenzurează materialul nostru.¹⁰⁴

De exemplu, publicația *New York Times* a cenzurat o telegramă care spunea că au fost distribuite milioane de dolari pentru influențarea anumitor cetățeni libieni cu legături politice, prin intermediul unor companii petroliere libiene. Telegrama nici măcar nu făcea referire la o anumită companie petrolieră – *New York Times* a editat pur și simplu sintagma „companii petroliere“. ¹⁰⁵ Cel mai flagrant caz este probabil citarea de către *New York Times* a unei telegrame de șaiszeci și două de pagini despre programul de rachete al Coreei de Nord și despre faptul dacă vânduseră sau nu rachete Iranului, telegramă din care *New York Times* s-a folosit de două paragrafe pentru a argumenta, într-un articol, teza că Iran

ar avea rachete care ar putea lovi Europa, în timp ce în alte părți ale telegramei se argumenta tocmai teza opusă.¹⁰⁶

The Guardian a editat o telegramă despre Iulia Timoșenko, fostul prim-ministru al Ucrainei, în care se menționa că și-ar ascunde banii la Londra.¹⁰⁷ A cenzurat afirmațiile conform cărora elita Kazahstanului, în general, ar fi coruptă – nici măcar o persoană nu era numită – și afirmația că ENI, compania energetică italiană cu sediul în Kazahstan, și British Gas ar fi corupte.¹⁰⁸ În esență, *The Guardian* a cenzurat cazurile în care o persoană bogată era acuzată de ceva, excepție făcând situațiile în care *The Guardian* avea ceva împotriva acelei persoane bogate.¹⁰⁹ Astfel, de pildă, într-o telegramă despre organizațiile criminale din Bulgaria apărea și numele unui personaj rus, iar *The Guardian* a dat impresia că întreaga telegramă era despre el, dar el era doar un singur personaj într-o listă lungă de organizații și persoane implicate în organizațiile criminale ale Bulgariei.¹¹⁰ *Der Spiegel* a cenzurat un paragraf despre Angela Merkel – nu din pricina unor violări ale drepturilor sale, ci din simple rațiuni politice.¹¹¹ Exemplele sunt multe.¹¹²

ANDY: Concepția noastră despre libertatea informației și fluxul liber al informației este într-un fel o concepție nouă și radicală, dacă ne uităm la întreaga planetă. Aș spune că nu e atât de diferită în Europa față de alte țări. Da, există unele țări care funcționează după un model democratic, ceea ce înseamnă că poți citi, poți înțelege și poate chiar ataca în instanță infrastructura cenzurii, dar asta nu înseamnă că cenzura nu există acolo, în vreme ce în țări ca Arabia Saudită sau China îți va fi foarte greu să o faci.

JULIAN: Experiența mea mi-a arătat că în Occident este doar mult mai sofisticată, prin caracterul vag și straturile din ce în ce mai obscure în care este învelit tot ce se întâmplă. Aceste straturi există pentru ca cenzura să poată fi ascunsă, negată. Vă puteți

închipui procesul cenzurii ca pe o piramidă. Piramidei îi iese doar vârful din nisip, iar lucrul ăsta e intenționat. Vârful este public – cazurile de calomnie, asasinările jurnaliștilor, camerele de fotografiat smulse de personalul militar și așa mai departe –, cenzura cunoscută, publică. Dar acesta este elementul cel mai mic. Următorul strat de sub vârf este format din toate persoanele care nu-și doresc să fie în vârf, care se autocenzurează pentru a nu ajunge acolo. Apoi, în următorul strat se află tot soiul de stimulente economice, sau stimulente sub forma patronajului care se oferă unor persoane pentru a scrie despre anumite subiecte. Următorul strat este economie pură – ce subiecte sunt avantajoase din punct de vedere economic, chiar și fără includerea factorilor economici din straturile superioare ale piramidei. Mai departe, următorul strat este format din prejudecățile cititorilor care au doar un anumit nivel de educație, deci care, pe de-o parte, pot fi manipulați ușor cu informații false, dar căroră, pe de altă parte, nici nu le poți spune ceva adevărat și prea sofisticat. Ultimul strat este distribuția – bunăoară, unii oameni pur și simplu nu au acces la informație într-o anumită limbă. Așadar, aceasta este piramida cenzurii. Ceea ce face *The Guardian* cu redactările Cablegate se află în cel de-al doilea strat.

Acum, genul acesta de cenzură poate fi negată, fie din cauză că are loc în ascuns, fie din cauză că nu există nici o instrucțiune de a cenzura o anumită afirmație. Jurnaliștilor rareori li se spune: „Nu scrie nimic despre asta” sau: „Nu scoate la tipar informația aceea”. Mai degrabă e subînțeles că se așteaptă de la ei să o facă, fiindcă înțeleg interesele celor cu care doresc să fie în relații bune sau de care doresc să se apropie. Dacă te porți cum se cade vei fi mângâiat pe cap și recompensat, iar dacă nu, nu vei fi recompensat. E cât se poate de simplu. Îmi place adeseori să dau exemplul acesta: cenzura pe față care se făcea în Uniunea Sovietică, cenzura despre care s-a vorbit atât de mult în Occident – agresorii care

veneau la miezul nopții și scoteau jurnaliștii din casele lor –, a fost decalată cu douăsprezece ore. Acum se așteaptă lumina zilei pentru a se sechestra casele jurnaliștilor, atunci când aceștia își pierd protectorul și nu-și mai pot plăti datoriile. Jurnaliștii sunt scoși afară din case, acestea fiindu-le luate. Societățile occidentale s-au specializat în spălarea cenzurii și în structurarea afacerilor celor puternici de așa manieră încât orice discurs public rămas care reușește să răzbească să fie prea slab pentru a afecta relațiile de putere ale unei societăți puternic fiscalizate, pentru că aceste relații sunt ascunse în straturi de complexitate și secrete.

ANDY: Jérémie a spus ceva despre pedo-naziști.

JACOB: Iarăși ne-am întors la pedo-naziști.

JÉRÉMIE: Doi călăreți într-unul singur.

ANDY: Chestiunea pedo-naziștilor rezumă argumentele Germaniei, poate chiar ale unei părți a Europei, în favoarea cenzurii. Germania nu-și dorea nici un fel de discursuri de incitare la ură pe internet din cauza istoriei sale și, desigur, dacă spui că e nevoie să restricționezi internetul din cauza pedofililor, vei putea face orice. De asemenea, a existat o circulară internă în Comisia Europeană referitoare la chestiunea reținerii de date care menționa: „Ar trebui să discutăm mai des despre pornografia infantilă și atunci oamenii vor fi de acord”.¹¹³

JULIAN: Poți vorbi și despre chestiunea asta puțin? Despre faptul că dacă vrem să cenzurăm un singur lucru, să spunem doar pornografia infantilă, atunci, pentru a cenzura pornografia infantilă, pentru ca ea să nu mai poată fi văzută, trebuie să supraveghem totul și pe toată lumea. E nevoie să construim infrastructura. Trebuie să construim un sistem de spionaj și cenzură în masă pentru a cenzura un singur lucru.

ANDY: Totul stă în detaliile mecanismului – așa-numitul sistem de precenzură din Germania te obligă să numești persoana care e responsabilă din punct de vedere legal pentru ceea ce publici. Deci, în linii mari, dacă publici ceva, fie că e pe o foaie de hârtie sau pe internet, fără să spui cine e responsabilul legal pentru conținut, ai încălcat deja legea. Asta înseamnă că aloci responsabilitatea, iar dacă cineva încalcă legea și distribuie, să spunem, pornografie infantilă sau discursuri care incită la ură, poți spune pur și simplu „În regulă, ne uităm care este adresa individului, îl prindem și scoatem lucrurile astea de pe internet“.

JULIAN: Adică îl cenzurăm pe cel care publică, nu pe cel care accesează.

ANDY: Da. Și se urmăresc doar anumite lucruri. Sunt de acord că nu orice lucru trebuie să poată fi accesat oricând, pentru că dacă mă uit la problemele legate de discursurile de incitare la ură, găsesc câteodată lucruri cu adrese private ale unor persoane și așa mai departe, lucruri care pot duce la situații cu care nu sunt de acord.

JULIAN: Dar, Andy, e un lucru foarte nemțesc. Pentru a putea face asta, pentru a stabili ce este acceptabil și ce nu, trebuie să existe o comisie, trebuie să numești persoane în acea comisie, trebuie să existe un întreg proces de numire în comisie...

ANDY: Da, avem toate rahaturile astea. Crimele Germaniei din cel de-al Doilea Război Mondial – pentru tot ceea ce au făcut naziștii, pentru fiecare proprietate pe care au sechestrat-o, au emis chitanțe, au făcut o listă. Totul era compus din acte birocratice. Poți foarte bine să spui că Germania a ucis fără motiv o grămadă de oameni – și este adevărat –, dar a făcut-o într-o manieră birocratică. Așa e Germania.

JULIAN: Ca cineva să decidă ce ar trebui cenzurat și ce nu, ai nevoie de două lucruri. În primul rând, trebuie să construiești infrastructura tehnică pentru a efectua cenzura. Trebuie să construiești o mașinărie națională de cenzură care să opereze eficient. Iar în al doilea rând, trebuie să ai o comisie și un aparat birocratic. Iar acea comisie nu poate să fie decât secretă, din cauză că întreaga mașinărie devine inutilă în cazul în care nu e secretă, și atunci ai justiție secretă.

ANDY: Știi ceva? Avem un principiu bun în Germania.

JACOB: Unul singur?

ANDY: Principiul este că dacă nu e realist ca o anumită lege să fie aplicată, atunci ea nu ar trebui să existe. Dacă o lege nu are noimă, bunăoară dacă interzici morile de vânt sau mai știu eu ce, atunci spunem „Haideți, fiți serioși, lăsați-o baltă“. Noi, cei de aici, suntem inspirați de internetul pe care îl știam noi când se maturiza, de fluxul liber al informațiilor, liber în sensul de nelimitat, neîngrădit, necenzurat, nefiltrat. Iar dacă aplicăm planetei Terra ceea ce înțelegem noi prin flux liber al informațiilor – și a fost aplicat, în mare măsură, întregii planete – vedem, desigur, că guvernele au fost afectate de lucrul acesta și vedem modul în care a fost aplicată puterea și modul în care a fost gestionată cenzura, fie că e precenzură, postcenzură sau ce știu eu ce fel de cenzură. Cu toții am aflat despre complicatele conflicte care apar. Întrebarea importantă este care e concepția noastră despre guvern sau despre viitorul unei Organizații Post-Guvernamentale – poate WikiLeaks este prima sau una dintre primele OPG-uri –, pentru că nu sunt sigur că guvernele sunt răspunsul corect la toate problemele acestei planete, cum ar fi cele legate de mediu.

JULIAN: Nici guvernele nu știu sigur care este hotarul între ce ține de guvern și ce nu. E un hotar neclar. Guvernele ocupă spațiu, dar WikiLeaks ocupă o parte din spațiul internetului. Spațiul internetului este încorporat în spațiul real, dar, din pricina gradului de complexitate dintre obiectul încorporat și încorporarea ca atare, nu este ușor, din perspectiva încorporării, să determinăm că obiectul este încorporat. Din acest motiv avem sentimentul acesta al ciberspațiului – că ar fi de fapt un alt tărâm care există pe undeva –, din cauza caracterului său indirect, complex și universal. Când citiți un fișier de pe internet într-o anumită locație este la fel ca a-l citi într-o altă locație sau în viitor – aceasta este universalitatea sa. Deci în sensul acesta, ca organizație care ocupă spațiul cibernetic și reușește să transmită informații în spațiul mai amplu în care e încorporat acesta, poate că suntem o organizație poststatală, din cauza lipsei controlului geografic.

Nu vreau să împing această analogie prea departe, din cauză că mă aflu sub arest la domiciliu. Este evident că forța coercitivă a statelor se aplică tuturor oamenilor noștri, oriunde au fost identificați. Dar restului presei îi place să afirme că am fi o organizație media în afara oricărui stat și are mare dreptate cu privire la importanța neapartenenței la vreun stat. Obişnuiam să spun mereu: „Ce credeți voi că e Newscorp? O mare multi-națională“. Dar, în ciuda acestui lucru, Newscorp este structurată de așa manieră încât se poate ajunge la componentele sale cheie, iar acesta este motivul pentru care a avut atât de mult de suferit aici, în Regatul Unit, în urma scandalului de hacking al telefoanelor, și motivul pentru care încearcă acum să se dea atât de bine pe lângă administrația SUA. Dar dacă activele unei organizații sunt în primul rând informațiile pe care le deține, atunci ea poate depăși granițele naționale într-un fel care este destul de greu de împiedicat, ca rezultat al criptografiei. Există un motiv bine întemeiat pentru care s-a ridicat o blocadă financiară împotriva

noastră – celelalte elemente ale organizației noastre sunt mult mai greu de eliminat.¹¹⁴

JACOB: Dacă e să vorbim despre asta în termeni utopici, ar trebui să ne întoarcem în timp puțin mai mult. Așadar, m-ai întrebat despre hărțuirea la care am fost supus, m-ai întrebat despre cenzura din Occident și am vorbit mai devreme despre programul de asasinări la comandă al lui Obama, despre care se afirmă că ar fi legitim din cauză că e la mijloc un proces, deci e considerat un proces echitabil.

JULIAN: Ei bine, un proces secret.

JACOB: Putem să ne întoarcem în timp și să legăm chestiunea asta și de John Gilmore. Unul dintre procesele intentate de John Gilmore în legătură cu dreptul său de a călători în anonim în Statele Unite s-a încheiat când Curtea a spus literalmente: „Uite, o să consultăm legea, care e secretă. O vom citi și vom afla, citind această lege secretă, dacă ai voie să faci lucrul pe care ai voie să-l faci“. Și au descoperit, după ce au citit legea secretă, că, de fapt, avea voie să-l facă, fiindcă ceea ce spunea legea secretă nu-i limita libertatea. Nu a aflat niciodată ce stipula legea secretă, iar mai târziu au schimbat *politicile* Administrației pentru Securitatea Transporturilor și ale Departamentului de Securitate Internă al SUA, ca reacție la victoria sa în acest proces, pentru că se pare că legea secretă nu era destul de restrictivă.¹¹⁵

JULIAN: Așa că au făcut-o și mai restrictivă?

JACOB: Practic, da, permițând legiferarea birocrăției. Dar este important să atragem atenția că programul asasinărilor la comandă, hărțuirea pe care o au de înfruntat oamenii la frontiere, cenzura online, cenzura pe care o implementează corporațiile la porunca vreunui guvern sau la porunca vreunei corporații, toate

aceste lucruri sunt legate unele de altele. Și totul se rezumă la faptul că statul are prea multă putere în fiecare din locurile în care vedem că apar aceste fenomene. Aceasta se întâmplă din cauză că puterea s-a concentrat în aceste zone și a atras persoane care abuzează de ea sau care fac presiuni pentru a se recurge la ea. Și chiar dacă se întâmplă câteodată să existe cazuri legitime, ceea ce se poate observa este că lumea ar fi mult mai bună dacă nu ar exista această centralizare, dacă nu ar exista tendința către autoritarism.

Occidentul nu este deloc un caz special în acest sens, pentru că se pare că dacă ai un țar al securității cibernetice, situația nu este atât de diferită față de cea a altor națiuni de acum cincizeci de ani, în care aveai un țar al forțelor de securitate internă. Construim același gen de structuri autoritare de control, care vor atrage persoane care vor abuza de ele, iar acesta este un lucru despre care ne place să pretindem că ar fi altfel în Occident. Nu este altfel în Occident, pentru că există un continuum al guvernării, de la autoritarism la libertarianism. Nu o spun în sensul partidelor politice americane, ci în acest sens: pe linia aceluși continuum, Statele Unite sunt foarte departe de URSS în multe, multe aspecte, dar sunt mult mai aproape de URSS decât e Christiania, cartierul autonom din inima orașului Copenhaga, în Danemarca.¹¹⁶ Și este chiar mai departe, cred eu, de o lume potențial utopică pe care am crea-o dacă am coloniza planeta Marte. Am vrea să îndepărtăm cât se poate de mult de totalitarism și de autoritarism ceea ce am putea construi pe Marte. Câtă vreme nu avem așa ceva, ceea ce avem sunt eșecuri.

JÉRÉMIE: Din nou, toate acestea sunt legate între ele. Când vorbim despre concentrarea puterii vorbim din nou despre arhitectură. Iar când vorbim despre cenzura internetului, este vorba despre centralizarea puterii de a determina ce se poate accesa și ce nu, și dacă cenzura guvernamentală, sau chiar cenzura privată, este

sau nu o putere necuvenită. Avem acest exemplu: site-ul nostru, *laquadrature.net*, a fost cenzurat în Regatul Unit de către Orange UK timp de câteva săptămâni. Se afla într-o listă de site-uri a căror accesare era interzisă de către Orange celor care au mai puțin de optsprezece ani. Poate că am menționat termenul de pornografie infantilă când ne-am opus tipului acestuia de legislație, sau poate că pur și simplu nu le plăcea de noi din cauză că ne opunem politicilor lor împotriva neutralității internetului, deoarece noi milităm pentru o lege care să le interzică să discrimineze comunicațiile utilizatorilor lor.¹¹⁷ Nu vom afla niciodată. Dar iată un actor privat care, sub formă de serviciu, se oferă să le ia oamenilor posibilitatea de a accesa anumite informații pe internet. Eu văd aici un risc major, în spatele puterii pe care o dăm, fie companiei Orange, fie guvernului Chinei sau mai știu eu cui.

JACOB: Să clarificăm ceva – când spui privat în Regatul Unit, vrei să spui că dețin fiecare linie, fiecare conexiune cu fibră optică și tot, sau folosesc și din resursele statului? Cum au fost autorizate oficial undele radio? Statul nu intervine deloc? Nu au o obligație să fie vigilenți*?

JÉRÉMIE: Există autorizare. Se schimbă arhitectura internetului, are loc o trecere de la o singură rețea universală la divizarea într-o serie de subrețele mici. Dar ceea ce discutăm noi de la început sunt probleme globale, fie că vorbim despre declinul sistemului financiar, fie că vorbim despre corupție, fie că vorbim despre geopolitică sau despre problema energetică sau despre mediu. Toate acestea sunt problemele globale cu care se confruntă omenirea în zilele noastre și încă avem un instrument în mâinile noastre, unul global, care ne permite să comunicăm mai

* În original, *duty of care*, termen juridic care indică obligația individului sau a unei organizații de a respecta un standard rezonabil de vigilență în timpul săvârșirii unor acțiuni care ar putea dăuna altor indivizi sau organizații. (n.tr.)

bine, să răspândim cunoașterea mai bine, să participăm mai bine la procesele politice și democratice. Ceea ce tind eu să cred este că un internet global, universal, este singurul instrument cu care am putea să abordăm aceste probleme globale, iar acesta este motivul pentru care această bătălie pentru libertatea internetului este bătălia cea mai importantă, cea în care avem cu toții responsabilitatea să luptăm.

ANDY: Sunt totalmente de acord că trebuie să ne asigurăm că internetul este înțeles ca o rețea universală caracterizată printr-un flux liber de informație; trebuie nu doar să definim lucrul acesta foarte limpede, ci și să dezvăluim numele acelor companii și acelor furnizori de servicii care furnizează ceva ce ei numesc internet, dar care de fapt este ceva complet diferit. Dar cred că încă nu am răspuns la întrebarea-cheie dincolo de această chestiune a filtrării. Vreau să vă dau un exemplu referitor la chestiunea la care cred că e nevoie să răspundem. Cu câțiva ani în urmă, acum vreo zece ani, am protestat împotriva introducerii pe piață de către Siemens a unor așa-numite software-uri pentru filtru smart. Siemens este una dintre cele mai mari companii de telecomunicații din Germania și furnizor de echipamente de spionaj. Și au vândut acest sistem de filtrare unor companii, astfel încât, de pildă, angajații să nu se poată uita pe site-urile sindicatelor pentru a se informa despre drepturile lor și așa mai departe. Dar au blocat și site-ul Clubului Chaos Computer, lucru care ne-a supărat. L-au desemnat ca având „conținut criminal” sau ceva de genul, lucru pentru care am intentat acțiuni în instanță. Dar la un târg am decis să organizăm un protest uriaș și să înconjurăm standul Siemens și să filtrăm oamenii care intră și ies. Dar chestia amuzantă era că am anunțat protestul pe site-ul nostru pentru a atrage cât mai mulți oameni prin internet, iar oamenii din standul Siemens habar n-aveau,

pentru că și ei foloseau software-ul de filtrare, așa că nu putuseră să citească avertismentul care era afișat acolo la vedere.

JULIAN: Pentagonul a instalat un sistem de filtrare, astfel încât orice e-mail trimis către Pentagon care conținea cuvântul WikiLeaks să fie filtrat. Și astfel, în cazul lui Bradley Manning, organele procuraturii au comunicat în timpul urmăririi penale cu persoane din afara armatei despre „WikiLeaks“, dar nu au văzut niciodată răspunsurile primite, din cauză că ele conțineau cuvântul „WikiLeaks“.¹¹⁸ Statul siguranței naționale ar putea să-și vină singur de hac.

ANDY: Ajungem astfel înapoi la întrebarea de bază: există ceva ce ar putea fi numit informație cu efect negativ? Adică, din punctul de vedere al societății, vrem să avem un internet cenzurat pentru că este mai bun pentru societate sau nu? Și chiar dacă am vorbi despre pornografia infantilă ai putea spune: „Stai puțin, pornografia infantilă evidențiază o problemă, și anume abuzul copiilor, iar pentru a putea rezolva problema trebuie să cunoaștem problema“.

JACOB: Așadar oferă dovezi ale infracțiunii.

JULIAN: Păi nu, oferă un lobby.

ANDY: Aceasta ar fi abordarea cea mai radicală, dar dacă vorbim despre naști sau mai știu eu ce, trebuie totuși să poți spune despre ce vorbim. Persoanele care au familie se vor întreba: „Păi nu ar fi mai bine ca societatea să filtreze lucrurile negative, astfel încât să rămânem cu cele pozitive, sau nu cumva lucrul acesta ne-ar limita capacitatea de a vedea problemele și de a le gestiona și de a le trata și de a le rezolva?“

JÉRÉMIE: Eu cred că tot timpul soluția este alta decât cenzura. Când vorbim despre pornografia infantilă nu ar trebui nici măcar

să folosim cuvântul pornografie – este reprezentarea unor scene infracționale de abuz al copiilor. Lucrul care trebuie făcut este să mergem la servere, să le scoatem din funcțiune, să identificăm persoanele care au urcat conținutul pe internet, pentru a identifica persoanele care l-au produs, acestea fiind cele care au abuzat copii. Iar de fiecare dată când există o rețea de oameni, o rețea comercială și așa mai departe, să arestăm acei oameni. Iar când adoptăm legi – și avem una în Franța care stipulează că o autoritate administrativă a Ministerului Afacerilor Interne decide care site-uri vor fi blocate – vom suprima orice interes al serviciilor de investigații de a găsi persoanele care fac ticăloșiile acestea, fiindcă spunem: „Oh, eliminăm pur și simplu accesul la conținutul negativ“, și e ca și cum am pune palma în fața ochilor cuiva care observă o problemă și am pretinde că am rezolvat-o. Deci, doar din acea perspectivă, cred că e de ajuns să descriem astfel lucrurile – în condițiile în care suntem cu toții de acord că ar trebui să eliminăm imaginile acelea de pe internet.

JACOB: Îmi pare rău, dar nu-mi găsesc deloc astâmpărul. Este foarte frustrant să ascult argumentul pe care îl susții. Îmi vine să vărs, fiindcă ceea ce tocmai ai făcut a fost să spui: „Vreau să-mi folosesc poziția de putere pentru a-mi impune autoritatea asupra altor persoane, vreau să șterg istoria“. Poate că sunt un extremist în acest caz – și în multe alte cazuri, sunt sigur –, dar am să fac niște afirmații îndrăznețe. Acesta este, de fapt, un exemplu de deserviciu făcut prin ștergerea istoriei. Am aflat, mulțumită internetului, că există în societate o epidemie a abuzării copiilor. Asta e ceea ce am aflat ca urmare a acestei probleme a pornografiei infantile – și cred că ar fi mai bine să o numim exploatare infantilă –, am văzut dovezile acestui fapt. Cred că ascunderea și eliminarea conținutului sunt o bătaie de joc, pentru că, de fapt, poți afla foarte multe despre societate în întregul ei. De pildă, poți

afla – și e clar că nu voi avea niciodată o carieră în politică după ce termin propoziția aceasta, dar trebuie să clarificăm chestiunea –, afli, de exemplu, cine sunt cei care produc acest conținut, și afli despre persoanele care le-au căzut victime. E imposibil ca oamenii să ignore problema. Înseamnă că trebuie să începi să cauți cauza care dă naștere acestui lucru, adică pe cei care exploatează copiii. Printr-o ironie, cred că unele tehnologii de supraveghere ar fi utile aici, pentru recunoașterea facială a celor implicați și pentru a urmări metadatele imaginilor. Dacă am elimina conținuturile acestea, asigurându-ne că trăim într-o lume în care e posibil să se șteargă unele lucruri și alte lucruri nu, creând aceste corpuri administrative însărcinate cu cenzura și cu elaborarea politicilor, am porni pe o pantă alunecoasă care, după cum am văzut, s-a îndreptat direct către drepturile de autor, și s-a îndreptat către multe alte sisteme.

Poate nu ar trebui să alegem calea cea mai ușoară doar pentru că este o cauză nobilă să vânăm aceste înregistrări, poate ar trebui, de fapt, să încercăm să găsim făptașii crimelor, poate ar trebui de fapt să încercăm să-i ajutăm pe cei care au fost victimizați, chiar dacă genul acesta de ajutor costă. Poate, în loc să ignorăm problema, ar trebui să privim în față faptul că societatea, în întregul său, are această mare problemă care se manifestă pe internet într-un mod anume.

E ca atunci când, de exemplu, Polaroid a scos pe piață camera Swinger (camera care făcea fotografii instant), iar oamenii au început să facă fotografii abuzive și cu aceste camere. Dar soluția nu este să distrugem un anumit mijloc sau să-l supunem unui control polițienesc. Soluția este să găsim dovezi pentru a urmări în instanță infracțiunile pe care acel mijloc le-a dezvăluit. Nu trebuie să șubrezim acel mijloc sau să mutilăm întreaga societate din cauza acestui lucru. Pentru că vorbim aici despre pornografia infantilă, hai să vorbim despre poliție. Poliția abuzează oamenii în mod

regulat într-o mulțime de țări. Probabil sunt mai mulți polițiști abuzivi pe internet decât distribuitori de pornografie infantilă.

JULIAN: Aproape sigur sunt mai mulți.

JACOB: Știm că există un număr „n” de polițiști în lume și știm că un număr „x” dintre aceștia au comis încălcări de ordin etic – de regulă violente. Dacă ne uităm, de pildă, doar la mișcarea *Occupy*, vedem acest lucru. Ar trebui oare să cenzurăm internetul din cauză că știm că unii polițiști sunt ticăloși? Ar trebui să mutilăm capacitatea poliției de a face bine?

JULIAN: Mai există și chestiunea revictimizării, care se întâmplă când, mai târziu, copilul, sau adultul, sau persoanele cu care e el în contact social văd imaginile din nou abuzului.

JACOB: Atât timp cât acei polițiști sunt online, sunt revictimizat.

JULIAN: Da, poți spune că a vedea o imagine în care ești bătut de un polițist este revictimizare. Eu aș susține că protejarea integrității arhivei istorice a lucrurilor care s-au întâmplat în lume este mai importantă; revictimizarea are loc, dar, oricum, instaurarea unui regim de cenzură capabil să elimine bucăți de istorie ar însemna să nu putem aborda problema din cauză că nu o putem vedea. În anii '90 am lucrat în calitate de consilier pe chestiuni legate de internet pentru niște polițiști însărcinați cu prinderea pedofililor în Australia, Unitatea Victoriană pentru Exploatarea Copiilor. Acești polițiști nu se bucurau de introducerea sistemelor de filtrare, din cauză că atunci când oamenii nu pot vedea că există pornografie infantilă pe internet, se elimină lobby-ul care asigură polițiștilor fondurile pentru a opri abuzul copiilor.

JÉRÉMIE: Lucrul cu care suntem cu toții de acord – și care cred că este cel mai important – este că până la urmă cea care contează

cu adevărat și cea spre care poliția ar trebui să-și îndrepte atenția este responsabilitatea individuală a persoanelor care produc conținutul, materiale despre abuzul copiilor și lucruri de genul acesta.

JACOB: Nu suntem de acord. Nu asta am spus.

JULIAN: Nu, Jérémie vorbește despre producere, nu despre publicare – e o diferență.

JACOB: Nu producerea conținutului este problema, de fapt. Aș vrea să fac doar o mică clarificare – dacă, de exemplu, ai abuzat de un copil și Andy a făcut o poză ca dovadă, nu cred că Andy ar trebui urmărit în instanță.

JÉRÉMIE: Nu, e vorba de cei care fac abuzul. Să fim serioși, e complicitate.

ANDY: Dar unii oameni abuzează de copil pentru a produce imaginile, nu-i așa?

JACOB: Bineînțeles.

ANDY: S-ar putea să existe și un aspect economic în chestiunea asta.

JACOB: Sunt în întregime de acord cu tine. Eu fac aici o distincție, și anume că dacă conținutul ca atare este o probă istorică și o dovadă a unei infracțiuni, este dovada unei infracțiuni foarte serioase, și nu ar trebui să pierdem niciodată din vedere faptul că există fenomenul revictimizării, dar prima victimizare este problema fundamentală, fie că există imagini ale ei sau nu.

JÉRÉMIE: Desigur. Asta vreau să spun.

JACOB: E aproape irrelevant dacă există sau nu imagini. Când există imagini, este foarte important să ne amintim că trebuie să avem în vedere țelul principal, și că scopul este să oprim răul, să oprim abuzul. Asta înseamnă, în mare parte, că trebuie să ne asigurăm că există dovezile și că există un stimulent pentru cei care au instrumentele potrivite să descopere faptașii acestor infracțiuni. Lucrul acesta este, cred eu, foarte important, iar oamenii pierd din vedere lucrul acesta fiindcă le este mai ușor să se prefacă că nu există, iar apoi să oprească imaginile și să spună că asta a oprit abuzul. Și nu e adevărat.

ANDY: Și problema este că acum foarte mulți oameni vor prefera, evident, soluția mai ușoară, din cauză că este foarte supărător să ne uităm la ceea ce se întâmplă cu adevărat în societate. Cred că ai o șansă să te ocupi de o problemă politică deoarece nu încerci să creezi o politică care să ignore problema sau care să o facă invizibilă. Într-o anumită privință, poate fi vorba de politică cibernetică, dar mai e vorba și de modul în care o societate abordează problemele, și am dubii mari că informațiile ar putea să facă rău în mod direct. Ține, desigur, de capacitatea de a filtra și e de asemenea adevărat că nu vreau să văd toate imaginile care există pe internet. Există unele care mi se par cu adevărat dezgustătoare și altele care îmi distrag atenția, dar același lucru este adevărat și despre oricare magazin video care pune la dispoziție filme fictive și urâte. Deci întrebarea este: sunt în stare să gestionez ceea ce văd și ceea ce procesez și ceea ce citesc? Aceasta este abordarea bazată pe filtrare. Wau Holland, fondatorul organizației Chaos Computer Club, a spus ceva amuzant: „Știi, filtrarea ar trebui făcută la nivelul utilizatorului final și la nivelul dispozitivului final al utilizatorului final.”¹¹⁹

JULIAN: Deci filtrarea ar trebui făcută de oamenii care primesc informația.

ANDY: Ar trebui făcută aici. Aici! (Arătând spre capul lui.)

JULIAN: În creier.

ANDY: În dispozitivul final al utilizatorului final, adică lucrul pe care-l ai între urechi. Acolo ar trebui să filtrezi și nu ar trebui ca filtrarea să fie făcută de guvern în numele poporului. Dacă poporul nu vrea să vadă unele lucruri, ei bine, nu e nevoie să le vadă, iar în zilele noastre trebuie să filtrezi multe lucruri oricum.

Confidențialitate pentru cei slabi, transparență pentru cei puternici

JULIAN: Andy, am vorbit recent cu președintele Tunisiei și l-am întrebat ce se va întâmpla cu arhivele de informații adunate în timpul domniei dictatorului Ben Ali – echivalentul tunisian al arhivelor Stasi – și a spus că, deși acestea sunt foarte interesante, agențiile de spionaj reprezintă o problemă, sunt periculoase și va trebui să le scoată din funcțiune una câte una. Dar în privința arhivelor, a crezut că ar fi cel mai bine pentru coeziunea societății tunisiene ca acestea să rămână secrete, ca să nu existe învinuiri. Erai tânăr în timpul căderii agenției Stasi în Germania de Est, poți vorbi puțin despre arhivele Stasi și despre ceea ce crezi tu în legătură cu dezvăluirea arhivelor de securitate?

ANDY: Germania are probabil cea mai bine documentată agenție de spionaj de pe planetă, sau cel puțin una dintre ele. Toate documentele provenind de la *Staatssicherheit*-ul Germaniei de Est – fiecare manual, document de procedură, document de antrenament, studiu intern – sunt în cea mai mare parte publice. „În cea mai mare parte” înseamnă că nu toate pot fi accesate ușor, dar multe dintre ele pot, iar guvernul german a creat o agenție care să se ocupe de arhive astfel încât cetățenii Germaniei să aibă dreptul să-și vadă dosarele Stasi.

JULIAN: Guvernul german a creat agenți BStU (die Bundesbeauftragte für die Stasi-Unterlagen), un mare distribuitor de dosare Stasi.

ANDY: Da, iar jurnaliștii pot aplica așa-numitele anchete de cercetare, care sunt probabil comparabile cu cererile de acces la informație [în concordanță cu Legea libertății informației], care le permit să studieze dosarele. Și există multe cărți și chiar manuale de comportament strategic ce arată felul în care Stasi făcea diverse lucruri. Cred, de fapt, că acesta este un lucru foarte bun de la care să putem învăța. Înțeleg că e un pic prea mult să ne așteptăm de la guvernul Tunisiei să publice toate dosarele personale alcătuite de fosta agenție de spionaj din cauză că președintele – actualul președinte – va trebui să se gândească la propriile sale dosare, și la cele ale aliaților săi și așa mai departe. Aceste agenții de informații nu respectă confidențialitatea, așa că poți avea dosare despre activitățile tale sexuale, telecomunicațiile tale, transferurile de bani, despre tot ceea ce ai făcut vreodată, lucruri care poate nu vrei să fie dezvăluite.

JULIAN: Ai urmărit situația cu Amn El Dawla, securitatea de stat din Egipt? Mii de oameni au intrat și au prădat arhivele în timp ce Amn El Dawla încerca să le ardă și să le distrugă și să le arunce la gunoi, și multe dosare au ieșit și au fost împrăștiate peste tot. Puteai cumpăra un dosar la piață cu 2 dolari și să-l urci pe internet. Lucrul ăsta nu a distrus societatea egipteană.

ANDY: Nu, tot ceea ce spun eu este că înțeleg oarecum de ce unii oameni nu vor ca dosarele lor să fie dezvăluite. Pot înțelege asta, dacă mă gândesc cum ar fi fost să trăiesc într-o țară în care s-au păstrat despre mine informații timp de patruzeci de ani și de fiecare dată când mergeam la toaletă se nota.

JULIAN: Dar există și analiza cost-beneficiu, nu? În opinia mea, turnător odată, turnător pe veci.

ANDY: Da, dar argumentul eticii hacker, în esență, este să folosești informații publice și să protejezi informații sau date private, și cred cu adevărat că dacă milităm pentru confidențialitate – și avem motive foarte bune să o facem – nu ar trebui să spunem doar că există un echilibru al lucrurilor aici. Putem face distincția. Nu trebuie să lăsăm totul pe mâna publicului.

JACOB: Dar păstrarea aceasta a secretului are un beneficiu care e asimetric. Hai să luăm o anumită distanță, și să privim obiectiv. În esență, pornești de la o premisă complet falsă, și anume de la ideea că datele sunt private atunci când sunt limitate, iar lucrul ăsta pur și simplu nu este adevărat. De pildă, dacă în țara mea un milion de oameni au autorizația să acceseze datele astea private...

JULIAN: 4,3 milioane...

JACOB: Cum poți numi datele acelea private? Problema este că nu sunt sută la sută secrete pentru toată lumea.

JULIAN: Sunt secrete pentru cei fără putere, deținute de cei puternici.

ANDY: Da, ai dreptate. Dar dacă ar fi să deschidem o întreagă arhivă...

JULIAN: S-a întâmplat în unele țări europene.

ANDY: Nu, nu știu de nici o țară în care să fi fost făcute publice toate dosarele.

JULIAN: Într-o măsură mai mare decât în Germania, s-a întâmplat în Polonia, de pildă.

ANDY: Se prea poate. Ce s-a întâmplat, de fapt, partea negativă a acordului pe care l-a făcut Germania, este că au folosit foști ofițeri ai Securității de Stat a Germaniei de Est pentru ca Stasi să administreze nu doar arhivele Stasi, ci și o parte a așa-numitei „Noi Germanii“, fosta parte de est, acum unificată. Există o relatare interesantă despre o companie care a câștigat licitația publică pentru a curăța clădirea în care erau păstrate arhivele. Compania a câștigat licitația doar pentru că a licitat cel mai puțin pentru același serviciu pentru care licitau și celelalte companii. După șase ani, organizația care administra arhiva a observat că angajase pentru curățarea arhivei o companie creată de fosta agenție de spionaj a Germaniei de Est.

JÉRÉMIE: A fost o relatare despre asta și pe WikiLeaks. Am citit-o. A fost foarte bună.¹²⁰

ANDY: WikiLeaks a publicat știrea exact despre asta, așa că ai dreptate atunci când spui că odată ce arhivele sunt create și sunt în mâinile unor ticăloși, e greu să vrei confidențialitate.

JULIAN: Totuși putem aborda o problemă mai amplă. Internetul a dus la o explozie a cantității de informație accesibilă publicului – este pur și simplu extraordinar. Funcția educativă este extraordinară. Pe de altă parte, oamenii vorbesc despre WikiLeaks și spun: „Uite, toate informațiile private ale guvernului sunt acum publice, guvernul nu mai poate ține nimic secret“. Eu spun că e o prostie. Spun că WikiLeaks e doar umbra unei umbre. În realitate, faptul că am produs peste un milion de cuvinte de informație și le-am dăruit publicului este doar o funcție a imensei explozii la nivelul cantității de materiale secrete care există. Și, de fapt, grupările puternice au acum o cantitate atât de vastă de materiale secrete încât face ca acea cantitate disponibilă public să pară minusculă, iar publicațiile WikiLeaks sunt doar o fracțiune a acestui

material deținut de privați. Când priviți echilibrul acesta dintre, pe de-o parte, oamenii puternici care știu despre fiecare tranzacție cu cardul de credit din lume, iar, pe de altă parte, oamenii care caută pe Google toate blogurile lumii și comentariile altor oameni, cum îl vedeți?

ANDY: Aș putea spune că este un lucru bun ca toate arhivele acestea să fie făcute accesibile, pentru că oamenii vor afla că dacă-și folosesc cardul de credit vor lăsa o urmă. Unora dintre oameni, dacă încerci să le explici lucrurile astea, li se vor părea foarte greu de înțeles și foarte abstracte. Le vor înțelege în momentul în care își vor citi dosarul.

JULIAN: Dacă deschizi arhiva contului tău de Facebook, care are 800 MB de informații despre tine.

ANDY: Știu că după căderea blocului estic, cancelarul german Helmut Kohl a vrut să unifice Germania, iar americanii i-au impus o condiție în cadrul așa-numitelor negocieri 2+4. Au spus că doreau ca telecomunicațiile Germaniei să rămână sub controlul lor, sub supravegherea lor, iar Kohl a crezut că nu este un lucru important, din cauză că nu a înțeles ce înseamnă supravegherea telecomunicațiilor. M-am întâlnit cu cineva din cabinetul său și acesta mi-a spus că cei din cabinet erau foarte nemulțumiți de decizia asta și într-un final au aranjat ca aproximativ 8 000 de pagini de transcrieri ale apelurilor sale telefonice făcute de Stasi să fie aduse în biroul său pe două cărucioare mici. Iar el a zis: „Hei, ce-i cu astea?” Și i-au răspuns că „Acestea sunt apelurile dumneavoastră telefonice din ultimii zece ani, inclusiv cele cu amantele dumneavoastră, cu soția dumneavoastră, cu secretara dumneavoastră și așa mai departe”. Așa că l-au făcut să priceapă ce înseamnă interceptarea de telecomunicații. Și, într-adevăr, aceste dosare ale securității chiar ajută oamenii să înțeleagă ce fac

agențiile de informații. Deci am putea milita pentru publicarea completă și dacă ar fi să votăm chiar acum, nu sunt sigur că m-aș opune.

JULIAN: Nu aș vrea să vorbim atât de mult despre chestiunea asta, din cauză că există evident și cazuri în care dacă investighezi mafia, ar trebui ca informațiile să rămână secrete pe durata investigației. Există și circumstanțe când lucrul ăsta ar putea fi văzut ca fiind legitim. Nu vreau să spun că este legitim ca tactică; vreau să spun că este inevitabil din punct de vedere politic. Există unele cereri atât de convingătoare din punct de vedere politic în favoarea sa – cum ar fi că „tipii ăștia au mai omorât și înainte, acum pun la cale o altă crimă” –, încât indiferent dacă crezi sau nu că interceptările ar trebui să existe, ele vor exista oricum. Nu poți câștiga bătaia asta politică. Dar acest tip de supraveghere tactică are avantajul că poate fi parțial reglementată și că daunele vor fi limitate la un număr minim de persoane. Când interceptarea tactică este folosită pentru aplicarea legii (nu pentru spionaj), ea este folosită cel mai des pentru colectarea de probe. Probele ajung la tribunal, deci devin publice. Deci poți, cel puțin câteodată, să monitorizezi puțin ce se întâmplă. Și poți interoga oamenii la tribunal despre cum a fost colectată acea informație și de ce ar trebui să presupunem că este validă. Poți s-o ții sub observație. Dar reglementarea interceptării strategice este complet absurdă. Ea este, prin definiție, interceptarea tuturor, deci ce fel de legislație putem elabora dacă premisa de la care se pornește este interceptarea tuturor?

JÉRÉMIE: Dezbaterea aceasta despre dezvăluirea completă a dosarelor mă duce cu gândul la gruparea cunoscută sub numele de LulzSec, care a publicat 70 de milioane de dosare de la Sony – toate datele utilizatorilor Sony – și puteai vedea toate adresele,

adresele de e-mail și parolele. Cred că erau până și detalii ale cardurilor de credit a 70 de milioane de utilizatori. Cum sunt un activist al drepturilor fundamentale, m-am gândit: „Ceva trebuie să fie în neregulă aici dacă, pentru a-ți argumenta poziția sau pentru a te amuza, faci publice datele personale ale oamenilor“. Nu mă simțeam deloc în largul meu văzând adresele de e-mail ale oamenilor din acele dosare. Am crezut cumva că acele persoane se distrau cu securitatea informatică și că ceea ce demonstau era că o companie cu puterea și notorietatea lui Sony nu e în stare să păstreze secretele utilizatorilor săi, iar faptul că acele 70 de milioane de utilizatori și-au căutat adresa de e-mail sau numele într-un motor de căutare și au găsit acest dosar i-a făcut imediat să-și dea seama: „Vai, ce-am făcut când am predat datele astea lui Sony? Ce înseamnă să dai date personale unei companii?“

JACOB: Iar apoi împușcă mesagerul.

Șobolanii de la Operă

JULIAN: Am trecut prin toate aceste scenarii pesimiste, așa că acum aș vrea să ne uităm la un scenariu potențial utopic. Avem radicalizarea tinerilor pe internet, iar acum tinerii care sunt pe internet ajung să reprezinte aproape majoritatea tinerilor. Pe de altă parte, avem niște încercări disperate de anonimizare și liberalizare a publicării, de eliminare a cenzurii – există o gamă largă de interacțiuni între stat și sectorul privat, care luptă împotriva acestui lucru –, dar, hai să presupunem că vom urma traiectoria pozitivă. Cum va arăta situația în acest caz?

JACOB: Cred că avem nevoie, fără excepție, de dreptul de a citi și de a vorbi liber, fără să existe excepție nici măcar în cazul unui singur om, fără nici o excepție, pentru a-l cita greșit pe Bill Hicks.¹²¹ El a vorbit despre lucrul ăsta referitor la educație, îmbrăcăminte și mâncare, dar de fapt la asta se rezumă totul: fiecare are dreptul să citească, fiecare are dreptul să vorbească liber. Aici sunt cuprinse și dreptul la exprimarea anonimă a opiniei, capacitatea de a face tranzacții cu diferite persoane fără să existe intervenții ale unor terți, capacitatea de a călători liber, capacitatea de a corecta datele tale din diferite sisteme. Să avem transparență și răspundere pentru fiecare sistem în care vedem că există orice fel de influență.

ANDY: Aș adăuga ideea că, odată cu creșterea numărului sistemelor de procesare a informației și a laturii lor reprezentate de rețea, și odată cu disponibilitatea unor unelte ca Tor și criptarea și așa mai departe, cantitatea datelor care poate fi suprimată este destul de mică, ceea ce înseamnă că asta e tot ce trebuie să facă guvernele, iar ele o știu bine. Știu bine că a opera în secret în zilele noastre înseamnă doar a opera în secret pentru o anumită perioadă, mai devreme sau mai târziu totul devenind public, iar acesta este un lucru bun. Aspectul acesta schimbă modul în care operează. Lucrul acesta înseamnă că știu că există o răspundere. De asemenea, înseamnă că introduc în mod forțat posibilitatea denunțării în interiorul unor întreprinderi, ca în cazul legii Sarbanes-Oxley, care cerea companiilor înregistrate la bursele din SUA să aibă o infrastructură care să permită tragerea semnalelor de alarmă, astfel încât persoanele care trebuie să semnaleze superiorilor lor comportamente infracționale sau de altă natură să aibă o modalitate de a o face fără să fie afectate în mod direct de cei pe care îi denunță.¹²² Deci e un lucru bun și va crea, pe termen lung, mai multe procese sustenabile.

JÉRÉMIE: Continuând ideea lui Jake, cred că trebuie să clarificăm pentru toată lumea faptul că un internet liber, deschis și universal este probabil cel mai important instrument pe care îl avem pentru a aborda problemele globale care sunt în joc, că a-l proteja este probabil una dintre sarcinile fundamentale care revin generației noastre și că atunci când cineva, undeva – fie că e guvernul sau o companie – restricționează capacitatea unor persoane de a accesa acest internet universal, tot internetul are de suferit. Omenirea întreagă este restricționată. Suntem martorii faptului că putem crește împreună costurile politice ale unei astfel de decizii, iar fiecare dintre cetățenii care accesează internetul liber poate împiedica un asemenea comportament. Începem să observăm că

în calitate de cetățeni ai rețelei avem putere în ceea ce privește deciziile politice și că putem face ca guvernele noastre și cei care sunt aleși să ne reprezinte să fie mai responsabili de ceea ce fac atunci când iau decizii proaste care ne afectează libertățile fundamentale și care afectează un internet liber, global și universal.

Așadar, cred că ar trebui să punem aceste lucruri în practică. Ar trebui să continuăm să propagăm cunoștințele despre cum să o facem. Ar trebui să continuăm să ne îmbunătățim modurile de acțiune, felul în care facem schimb de tactici în ceea ce privește intervențiile în parlament, demascarea politicienilor, demascarea influenței pe care o au lobby-urile industriale asupra procesului de elaborare de politici. Ar trebui să continuăm să construim instrumente care să le permită cetățenilor să-și construiască propriile infrastructuri descentralizate și criptate, să le permită să dețină propria infrastructură de comunicații. Ar trebui să promovăm aceste idei în întreaga societate ca o modalitate de a clădi o lume mai bună și deja începem să o facem – trebuie doar să continuăm.

JULIAN: Jake, dacă te uiți la descrierea problemelor internetului făcută de persoane ca Evgeny Morozov, aceste probleme au fost prevăzute acum mult timp de către membrii mișcării cypherpunk.¹²³ Ei nu erau de părere că trebuie doar să ne plângem de statul polițienesc care începea să înmugurească, ci că putem, că trebuie chiar, să construim uneltele unei noi democrații. Le putem construi de fapt cu mintea, le putem distribui altor oameni și putem să ne construim, împreună, apărarea. Tehnologia și știința nu sunt neutre. Există anumite forme de tehnologie care ne oferă aceste drepturi și libertăți fundamentale la care au sperat atât de mulți, de atât de multă vreme.

JACOB: Desigur. Cred că lucrul fundamental cu care ar trebui să rămânem – mai cu seamă în cazul cuiva de șaisprezece sau

optsprezece ani care și-ar dori să facă din lume un loc mai bun – este că nici unul dintre cei care suntem aici și nimeni în lumea aceasta nu s-a născut cu realizările care le vor fi mai târziu inscripționate pe mormânt. Cu toții construim alternative. Toți cei care suntem aici de față am construit alternative și fiecare, mai ales mulțumită internetului, are puterea să facă acest lucru în privința contextului în care trăiește. Și nu că ar avea o datorie de a o face, dar dacă e să-și dorească acest lucru, o poate face. Și dacă o face, va avea un impact asupra multor oameni, mai ales în ceea ce privește internetul. Construirea acelor alternative implică o amplificare, o augmentare.

JULIAN: Așadar, dacă construiești un lucru, îl poți oferi unui miliard de oameni pentru a-l folosi.

JACOB: Sau dacă participi la construirea unei rețele a anonimității – cum e rețeaua Tor, bunăoară – ajuți la construirea alternativei comunicației anonime unde înainte ea nu exista.

JÉRÉMIE: Este distribuirea liberă a cunoașterii și prilejuirea unor canale de comunicație prin care cunoașterea să treacă liber, asta este ceea ce faci. Tor este un software liber, care este astăzi atât de răspândit pentru că înglobăm acea noțiune de libertate în modul în care construim alternative, în care construim tehnologii, în care construim modele.

JACOB: Avem nevoie de software liber pentru o lume liberă, și avem nevoie de hardware liber și cu sursă deschisă.

JULIAN: Dar prin liber înțelegi neîngrădit, oamenii se pot juca cu elementele interne, pot vedea cum funcționează?

JACOB: Întocmai. Avem nevoie de software care este la fel de liber ca legile unei democrații, astfel încât fiecare să-l poată studia,

schimba, să-l poată înțelege în întregime și să se asigure că acel software face ceea ce-și dorește utilizatorul să facă. Software Liber, Hardware Liber și cu Sursă Deschisă.¹²⁴

JULIAN: Cei din mișcarea cypherpunk au avut această idee că „codul este lege”.

JÉRÉMIE: Ideea e a lui Larry Lessig.

JULIAN: Pe internet, ceea ce poți face este definit de tipul programelor care există, de tipul programelor care rulează, deci codul este lege.

JACOB: Foarte adevărat, iar acest lucru înseamnă că poți construi alternative, mai cu seamă în ceea ce privește scrierea de programe, dar chiar și în ceea ce privește imprimarea 3D sau chestii sociale precum locațiile hackerspace care există.¹²⁵ Poți ajuta la construirea alternativelor, iar ceea ce este cel mai important este ca ele să intre într-un proces de normalizare, unul în care oamenii să se obișnuiască, din punct de vedere social, cu construirea propriilor obiecte 3D, cu modificarea software-ului propriu, și unul în care sunt conștienți că dacă cineva îi împiedică să facă acest lucru, atunci acel cineva nu furnizează acces la internet, ci furnizează un internet filtrat, cenzurat și, de fapt, își încalcă obligația de a purta de grijă.

Asta e ceea ce fiecare dintre noi a făcut cu viața sa, iar oamenii ar trebui să știe că au posibilitatea să o facă pentru generațiile viitoare, și pentru generația de acum. De asta mă aflu aici – pentru că dacă nu-l susțin acum pe Julian, în toate lucrurile prin care trece, ce fel de lume aș mai construi? Ce fel de mesaj transmit lumii când permit unor porci să mă intimidizeze? În nici un caz, niciodată. Trebuie să construim și să schimbăm situația asta. După cum a spus Ghandi: „Fii tu însuși schimbarea pe care vrei să

o vezi în lume⁴, dar trebuie să fii și tulburarea pe care vrei să o vezi în lume.¹²⁶ E un citat din *A Softer World*, nu e același cu citatul lui Ghandi, dar cred că oamenii trebuie să știe că nu pot să stea pur și simplu deoparte, neimplicați, ci trebuie să ia atitudine, și sper că o vor face.¹²⁷

ANDY: Cred că există o bună șansă ca oamenii să continue lucrurile din punctul în care le-am adus noi, iar alternativele vin din partea oamenilor care nu sunt mulțumiți de situația pe care o găsesc sau de opțiunile pe care le au.

JULIAN: Poți vorbi puțin și despre Chaos Computer Club în acest conținut?

ANDY: Mereu CCC ăsta.¹²⁸

JULIAN: Păi e unic în lume.

ANDY: CCC este o organizație galactică de hackeri care promovează libertatea accesului la informație, transparența tehnologiei și care se preocupă de relația dintre dezvoltarea umană și cea tehnologică, așadar de interacțiunea dintre societate și tehnologie.

JULIAN: A devenit, de fapt, politică.

ANDY: CCC a devenit un soi de forum al hacking-ului, cu câteva mii de membri aflați oarecum în Germania – dar noi nu considerăm că locuim în Germania, noi considerăm că locuim pe internet, ceea ce reprezintă, poate, o parte importantă a imaginii noastre de sine, care exercită farmecul ei. Suntem foarte bine conectați la alte grupuri de hackeri din Franța, America și din alte țări.

JULIAN: Și de ce crezi că a apărut în Germania? Nucleul este în Germania – de-aici s-a extins în restul lumii.

ANDY: Nemții încearcă tot timpul să structureze totul.

JÉRÉMIE: Ingineria nemțească e mai bună.

JULIAN: Dar cred că nu este doar asta. E vorba despre Berlin, și despre căderea blocului estic.

ANDY: Are de-a face cu mai multe lucruri. Germania a făcut cel mai rău lucru pe care îl poate face o țară altor oameni, deci e poate puțin mai imună la repetarea acelor lucruri – lucruri precum intrarea în război cu alte țări. Am făcut toate aceste lucruri, am trecut prin asta, am fost pedepsiți aspru și a trebuit să învățăm de pe urma acestei experiențe, iar felul acesta descentralizat de a gândi și comportamentul antifascist, cum ar fi prevenirea unui stat totalitar, încă sunt predate în școlile Germaniei din cauză că am avut experiența acelor lucruri la cel mai rău nivel. Deci cred că, în parte, așa ar trebui să înțelegem CCC-ul, care este oarecum un fenomen german. Wau Holland, cel care a fondat CCC, a avut și o abordare foarte pronunțat politică în privința sa. L-am întâlnit la mormântul lui Wau pe tatăl său, deoarece fiul a murit înaintea sa, iar tatăl său nu a avut de spus cuvinte plăcute. A spus: „...și ca niciodată să nu mai existe activități totalitare, antipacifiste pe teritoriul german“. Acesta a fost comentariul tatălui când și-a îngropat fiul, iar acest lucru mi-a lămurit multe despre motivul pentru care Wau a fost atât de hotărât să influențeze oamenii și să aibă grijă de ei, să se comporte în mod pașnic cu ceilalți, răspândind idei, nu limitându-le, fără să fie agresiv, ci cooperant.

Iar ideea creării în mod cooperant a unor lucruri – cum ar fi mișcările pentru sursă deschisă – a infectat într-adevăr ideile mișcării cypherpunk americane și s-a unit cu ele și cu cele ale lui Julian Assange/WikiLeaks și așa mai departe. Ceea ce se întâmplă acum este ceva global, și există atitudini culturale foarte diferite, foarte descentralizate, ale unor hackeri elvețieni, germani, italieni – iar acesta este un lucru bun. Hackerii italieni

se comportă complet diferit față de hackerii germani – oriunde ar fi, trebuie să gătească bine; hackerii germani trebuie să aibă totul bine structurat. Nu spun că unii sunt mai buni decât ceilalți, vreau doar să spun că fiecare dintre aceste culturi descentralizate are părțile ei foarte frumoase. La conferința hackerilor italieni poți merge în bucătărie și vei vedea acolo un loc minunat; la tabăra germană de hacking vei găsi un internet minunat, dar ai face bine să nu te uiți în bucătărie. Oricum, esența lucrurilor este că noi creăm. Și cred că ne aflăm într-un soi de conștiință comună care este cât se poate de îndepărtată față de identitatea noastră națională – aceea de nemți sau italieni sau americani sau mai știu eu ce –, vedem doar că ne dorim să rezolvăm problemele, ne dorim să lucrăm împreună. Vedem această cenzură a internetului, această luptă a guvernelor împotriva tehnologiilor noi, ca pe un soi de situație evolutivă pe care trebuie să o depășim.

Și suntem pe cale să identificăm și soluții, nu doar probleme, ceea ce e bine. Probabil că încă va trebui, în următorii cine știe câți ani, să luptăm împotriva multor tâmpenii, dar acum, în sfârșit, a apărut o generație de politicieni care nu văd internetul ca pe un dușman, ci înțeleg că el face parte din soluție, nu din problemă. Lumea noastră încă este construită pe armament, pe puterea secretelor, pe un întreg cadru economic și așa mai departe, dar lucrul acesta se schimbă și chiar cred că jucăm un rol foarte important în procesul actual de elaborare de politici. Putem discuta despre aceste probleme într-o manieră controversată – iar acesta este un lucru pe care CCC-ul a reușit să-l facă de multă vreme încoace. Nu suntem un grup omogen, avem opinii foarte diferite. Îmi place că stăm aici împreună și că nu formulăm cele mai bune răspunsuri imediat, formulăm mai degrabă întrebări și ne punem fiecare ideile la bătaie și vedem care e concluzia. Acesta este genul de proces care trebuie să continue, iar pentru aceasta avem nevoie de un internet liber.

JULIAN: M-am întrebat care ar fi traiectoria pozitivă pentru viitor. Autocunoaștere, diversitate și rețele de autodeterminare. O populație globală educată – nu vreau să spun educată în mod formal, ci educată în sensul înțelegerii felului în care funcționează civilizația omenească la nivel politic, industrial, științific și psihologic – ca rezultat al schimbului liber de comunicații, stimulând de asemenea culturi noi și pline de viață și diversificarea maximă a gândirii individuale, autodeterminare regională sporită și autodeterminare a grupurilor de interese care pot să interacționeze repede și pot face schimb de valori rapid, peste hotarele geografice. Și poate că lucrurile acestea și-au găsit expresia în Primăvara Arabă și în activismul panarab care a fost amplificat de internet. În cadrul colaborării noastre cu Nawaat.org, cei care au creat Tunileaks, eliberând de sub cenzura regimului telegramele departamentului de stat din Tunisia prereroluționară, am văzut din proprie experiență puterea pe care o are rețeaua de a trimite informația acolo unde este necesară, și a fost o recompensă uriașă faptul de a mă fi aflat, mulțumită eforturilor noastre, în poziția de a putea contribui la ceea ce începea să se întâmple acolo.¹²⁹ Nu văd acea luptă pentru autodeterminare ca fiind diferită de a noastră.

Această traiectorie pozitivă ar impune cunoașterea de sine a civilizației umane, deoarece trecutul nu poate fi distrus. Ar însemna imposibilitatea apariției statelor neo-totalitare, datorită mișcării libere a informației, capacitatea oamenilor de a vorbi în privat unii cu alții și de a conspira împotriva unor astfel de tendințe și capacitatea microcapitalului de a se scurge fără a fi controlat din astfel de locuri ostile oamenilor.

Pe aceste fundații poate fi construită o gamă largă de sisteme politice. Pentru mine utopia ar fi o distopie dacă ar fi doar una. Sunt de părere că idealurile utopice trebuie să însemne o diversitate de sisteme și de modele de interacțiune. Dacă ar fi să ne uităm la

dezvoltarea efervescentă a unor noi produse culturale și chiar la schimbarea lingvistică, la subculturi care-și elaborează propriile mecanisme de interacțiune alimentate de internet, atunci pot spune că da, această cale pozitivă pare să se deschidă.

Dar cred că, cel mai probabil, tendințele spre omogenizare, universalitate, spre transformarea întregii civilizații omenști într-o singură piață vor aduce, pentru fiecare serviciu sau produs, factori normali de piață, cum ar fi un lider de piață, un al doilea, un al treilea jucător – care va fi unul de nișă, iar apoi niște codași care nu au nici un cuvânt de spus. Cred că aceasta ar putea să aducă o masivă omogenizare lingvistică, o masivă omogenizare culturală, o standardizare masivă pentru a face ca aceste schimbări rapide să fie eficiente. Deci cred că scenariul pesimist este de asemenea probabil, iar statul polițienesc transnațional și nesfârșitele războaie cu dronă se apropie și ele.

De fapt, îmi amintesc de o seară în care m-am furișat la teatrul de operă din Sydney pentru a vedea piesa *Faust*. Opera din Sydney este foarte frumoasă pe timp de noapte, cu interiorul său măreț și luminile strălucind peste apă, spre cerul înstelat. După spectacol, am ieșit afară și am auzit trei doamne care discutau, aplecate pe balustrada care domina golful întunecat. Doamna mai în vârstă vorbea despre problemele pe care le avea la locul de muncă, loc care s-a dovedit a fi la CIA, un post de agent secret, și despre faptul că se plânsese la Comisia de Informații a Senatului SUA și așa mai departe, și spunea toate aceste lucruri, în șoaptă, nepoatei sale și unei alte doamne. Și m-am gândit: „Deci e adevărat. Agenții CIA chiar își petrec timpul la teatrul de operă din Sydney!” Și apoi m-am uitat în interiorul operei prin uriașele panouri de sticlă ale fațadei, iar acolo, în tot acel rafinament somptuos și solitar, era un șobolan de apă care se furișase în interiorul operei și care alerga încoace și-ncolo, sărind pe mesele acoperite cu pânză fină și ciugulind din mâncarea Operei, sărind pe ghișeul unde erau

toate biletele și simțindu-se de minune. Și cred că acesta este cel mai probabil scenariu pentru viitor: o structură extrem de restrictivă, omogenizată, postmodernă, transnațională și totalitară de o complexitate de necrezut, absurdă și devalorizată, iar în interiorul acestei complexități incredibile, un spațiu în care pot ajunge doar șobolanii isteți.

Acesta este un aspect pozitiv al unei traiectorii negative, traiectoria negativă fiind un stat polițienesc transnațional, ticsit cu drone, un neofeudalism în rețea al elitei transnaționale – nu în sensul clasic al cuvântului, ci în sensul unei interacțiuni complexe, multipartite, care a apărut ca urmare a delimitării mai multor elite naționale față de populația comună și a unirii între ele a acestor elite. Toate comunicațiile vor fi supravegheate, stocate pe veci, urmărite în permanență, fiecare individ, în toate interacțiunile sale, va fi identificat ca acel individ, de la naștere până la moarte, de către aceste noi cercuri conducătoare. Aceasta este o schimbare majoră, chiar în raport cu ceea ce era acum zece ani, și practic suntem deja acolo. Cred că acest lucru nu poate produce decât o atmosferă de control strict. Dacă toate informațiile care au fost adunate despre lumea în care trăim ar fi publice, acest lucru ar putea reechilibra dinamica puterii și ne-ar permite, în calitate de civilizație globală, să ne modelăm propriul destin. Dar fără o schimbare dramatică acest lucru nu se va întâmpla. Supravegherea în masă se aplică, în proporții diferite, celor mai mulți dintre noi, transferând putere către cei din interiorul sistemului care însă, cred eu, nu se vor bucura nici ei prea mult de această minunată lume nouă. Acest sistem va coincide și cu o cursă a înarmării cu drone care va elimina hotarele clar definite așa cum le știm astăzi, fiindcă aceste hotare sunt rezultatul contestării unor delimitări fizice, iar rezultatul va fi un război perpetuu în care rețelele de influență victorioase vor începe să stoarcă concesiile de la lume.

Iar pe lângă aceasta, oamenii vor fi pur și simplu îngropați sub imposibila matematică a birocrăției.

Cum poate o persoană normală să fie liberă într-un astfel de sistem? Pur și simplu nu poate, este imposibil. Nu că am putea fi complet liberi vreodată, în orice sistem, dar libertățile pentru care am evoluat din punct de vedere biologic și libertățile cu care ne-am obișnuit din punct de vedere cultural vor fi eliminate aproape în întregime. Deci cred că singurii oameni care vor reuși să-și păstreze libertatea pe care am avut-o, să spunem, acum douăzeci de ani – pentru că sistemul de supraveghere a eliminat deja o mare parte a ei, noi pur și simplu nu ne dăm seama încă – vor fi cei care vor fi educați în ceea ce privește funcționarea internă a sistemului. Prin urmare, doar o elită de rebeli high-tech va rămâne liberă, acești șobolani isteți care fug prin clădirea Operei.

Note

1. Simplu spus, criptografia, provenind de la termenul grecesc care înseamnă „scriere secretă”, este practica comunicării codate.
2. „Oxford English Dictionary Updates Some Entries & Adds New Words; Bada-Bing, Cypherpunk, and Wi-Fi Now in the OED”, ResourceShelf, 16 septembrie 2006: <http://web.resourceshelf.com/go/resourceblog/43743> (accesat în data de 24 octombrie 2012)
3. WikiLeaks: <http://wikileaks.org>
4. Pentru mai multe informații despre fișierul *Rubberhose*, vezi: „The Idiot Savants’ Guide to Rubberhose”, Suelette Dreyfus: <http://marutukku.org/current/src/doc/maruguide/t1.html> (accesat în 14 octombrie 2012)
5. Pentru mai multe informații despre cartea *Underground*, vezi <http://www.underground-book.net>
Pentru mai multe informații despre filmul *Underground: The Julian Assange Story*, vezi: „The Internet Movie Database”: <http://www.imdb.com/title/tt2357453/> (accesat în data de 21 octombrie 2012)
6. Noisebridge este un spațiu virtual pentru hacking, cu baza în San Francisco, și furnizor de infrastructură pentru proiecte tehnico-creative, condus colaborativ de membrii săi: <https://www.noisebridge.net/wiki/Noisebridge>
Chaos Computer Club din Berlin este ramura din Berlin a Chaos Computer Club (mai multe informații la adresa): https://berlin.ccc.de/wiki/Chaos_Computer_Club_Berlin.
7. Proiectul Tor: <https://www.torproject.org>
8. Chaos Computer Club este cea mai mare asociație de hacking din Europa. Activitățile sale variază de la cercetare și explorare de natură tehnică până la campanii, evenimente, publicații și consultanță politică: <http://www.ccc.de>.
9. EDRI: <http://www.edri.org>

10. ICANN: <http://www.icann.org>
11. buggedplanet: <http://buggedplanet.info>
12. Cryptophone: <http://www.cryptophone.de>
13. La Quadrature du Net: <http://www.laquadrature.net>
14. Collateral Murder: <http://www.collateralmurder.com>
 The Iraq War Logs: <http://wikileaks.org/irq>
 The Afghan War Diary: <http://wikileaks.org/afg>
 Cablegate: <http://wikileaks.org/cablegate.html>
15. „Congressional committee holds hearing on national security leak prevention and punishment“, Reporters Committee for Freedom of the Press, 11 iulie 2012: <http://www.rcfp.org/browse-media-law-resources/news/congressional-committee-holds-hearing-national-security-leak-prevent> (accesat în data de 21 octombrie 2012).
16. Pentru mai multe informații despre Marele Juriu pentru WikiLeaks, vezi lista cronologică a jurnalistei freelance Alexa O'Brien la: http://www.alexao'Brien.com/timeline_us_versus_manning_assange_wiki-leaks_2012.html (accesat în data de 22 octombrie 2012).
17. „Bradley Manning's treatment was cruel and inhuman, UN torture chief rules“, *Guardian*, 12 martie 2012: <http://www.guardian.co.uk/world/2012/mar/12/bradley-manning-cruel-inhuman-treatment-un> (accesat în data de 24 octombrie, 2012).
18. „WikiLeaks: guilty parties «should face death penalty»“, *Telegraph*, 1 decembrie 2010: <http://www.telegraph.co.uk/news/worldnews/wikileaks/8172916/WikiLeaks-guilty-parties-should-face-death-penalty.html> (accesat în data de 22 octombrie, 2012).
19. „CIA launches task force to assess impact of U.S. cables' exposure by WikiLeaks“, *Washington Post*, 22 decembrie 2012: <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/21/AR2010122104599.html?hpid=topnews&sid=ST2010122105304> (accesat în data de 22 octombrie 2012).
20. „WikiLeaks fights to stay online after US company withdraws domain name“, *Guardian*, 3 decembrie 2012: <http://www.guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns> (accesat în data de 23 octombrie 2012).
21. „Don't Look, Don't Read: Government Warns Its Workers Away From WikiLeaks Documents“, *New York Times*, 4 decembrie 2010: http://www.nytimes.com/2010/12/05/world/05restrict.html?hp&_r=2& (accesat în data de 23 octombrie 2012).

22. „Banking Blockade“, WikiLeaks: <http://www.wikileaks.org/Banking-Blockade.html> (accesat în data de 22 octombrie 2012).
23. Relatarea scrisă a reținerilor lui Jacob este o lectură recomandabilă. Vezi: „Air Space — a trip through an airport detention center“, boingboing, 31 octombrie 2011: <http://boingboing.net/2011/10/31/air-space-a-trip-through-an-ai.html>
De asemenea, este important în acest sens și un interviu cu Jacob despre reținerile sale, acordat publicației *Democracy Now*: „National Security Agency Whistleblower William Binney on Growing State Surveillance“, *Democracy Now*, 20 aprilie 2012: http://www.democracynow.org/2012/4/20/exclusive_national_security_agency_whistleblower_william (ambele linkuri au fost accesate în data de 13 octombrie 2012).
24. În mod oficial, cazul este cunoscut ca In the Matter of the 2703(d) Order Relating to Twitter Accounts [Chestiunea Ordinului 2703(d), referitor la conturile Twitter]: Wikileaks Rop_G IOERROR; și Birgitta].
25. „Secret orders target e-mail“, *Wall Street Journal*, 9 octombrie 2011: <http://online.wsj.com/article/SB10001424052970203476804576613284007315072.html> (accesat în data de 22 octombrie 2012).
26. „Twitter Ordered to Yield Data in WikiLeaks Case“, *New York Times*, 10 noiembrie, 2011: https://www.nytimes.com/2011/11/11/technology/twitter-ordered-to-yield-data-in-wikileaks-case.html?_r=1 (accesat în data de 22 octombrie 2012).
27. „ACLU and EFF to Appeal Secrecy Ruling in Twitter/WikiLeaks Case“, *Electronic Frontier Foundation*, 20 ianuarie 2012: <https://www.eff.org/press/releases/aclu-eff-appeal-secrecy-ruling-twitter-wikileaks-case> (accesat în data de 22 octombrie 2012)
28. Este vorba despre protestul din 6 aprilie 2008, organizat pentru a susține greva înăbușită a muncitorilor de la fabrica de textile Mahalla al-Kobra. Cu puțin timp înaintea protestului, „Mișcarea Tinerilor 6 Aprilie“ s-a format ca grup pe Facebook, conceput pentru a încuraja oamenii să protesteze în Cairo și în alte orașe pentru a coincide cu acțiunea industrială din Mahalla. Protestele nu au mers conform planului, iar administratorii grupului de Facebook, Esraa Abdel Fattah, Ahmed Rashid și Ahmed Maher au fost arestați, împreună cu alții. Maher a fost torturat pentru parola contului său de Facebook. Mișcarea Tinerilor 6 Aprilie a jucat un rol și în revoluția egipteană din 2011. Vezi: „Cairo Activists Use Facebook to Rattle Regime“, *Wired*, 20 octombrie 2008: http://www.wired.com/techbiz/startups/magazine/16-11/ff_facebook-egypt?current-Page=all (accesat în data de 23 octombrie 2012).

29. „Cum să protestezi inteligent“, autori anonimi, distribuit la începutul revoluției de optsprezece zile care l-a înlăturat de la putere pe președintele Mubarak (varianta în arabă): <http://www.itstime.it/Approfondimenti/Egyptian-RevolutionManual.pdf>. Fragmente din acest document au fost traduse și în engleză și publicate la: „Egyptian Activists' Action Plan: Translated“, *Atlantic*, 27 ianuarie 2011: <http://www.theatlantic.com/international/archive/2011/01/egyptian-activists-action-plan-translated/70388> (ambele linkuri au fost accesate în data de 23 octombrie 2012).
30. Panopticonul este o închisoare inventată de filosoful Jeremy Bentham în 1787, proiectată în așa fel încât să permită unui singur gardian să supravegheze toți prizonierii în același timp, pe ascuns, privindu-i. Jeremy Bentham (editat de Miran Bozovic), *The Panopticon Writings* (Verso, 1995), disponibil online la: <http://cartome.org/panopticon2.htm> (accesat în data de 22 octombrie 2012).
31. Johannes Gutenberg (1398–1468) a fost un fierar german care a inventat tiparul cu caractere mobile, o invenție care a dus la unele dintre cele mai semnificative schimbări sociale din istorie. Invenția presei de tipar este corespondentul istoric cel mai apropiat al invenției internetului.
32. John Gilmore este unul dintre primii cypherpunks, unul dintre fondatorii Electronic Frontier Foundation și activist pentru libertățile civile. Fraza citată de Andy a fost citată prima dată în „First Nation in Cyberspace“, *Time Magazine*, 6 decembrie 1993. Vezi site-ul lui John Gilmore: <http://www.toad.com/gnu> (accesat în data de 22 octombrie 2012).
33. „Tehnologia proprietară este orice fel de sistem, instrument sau proces tehnic care este dezvoltat de și pentru o afacere anume [...] Ideile dezvoltate și predate de către angajați sunt considerate de obicei proprietatea intelectuală a angajatorului, lucru care le permite să se numească tehnologii proprietare.“ Definiție preluată de la wiseGEEK: <http://www.wisegeek.com/what-is-proprietary-technology.htm> (accesat în data de 22 octombrie 2012).
34. Cory Doctorow, „The coming war on general-purpose computing“, boingboing, 10 ianuarie 2012 (bazat pe un discurs important ținut la Chaos Computer Congress, în decembrie 2011): <http://boing-boing.net/2012/01/10/lockdown.html> (accesat în data de 15 octombrie 2012).
35. Stuxnet este un virus de calculator foarte sofisticat, despre care se crede că a fost elaborat de SUA și Israel pentru a ataca echipamentul Siemens despre care se presupunea că ar fi folosit de Iran pentru îmbogățirea uraniului. Pentru o expunere de ansamblu, vezi Wikipedia: <http://en.wikipedia.org/wiki/Stuxnet>. Vezi, de asemenea, „WikiLeaks: US advised to sabotage Iran

nuclear sites by German thinktank“, *Guardian*, 18 ianuarie 2011: <http://www.guardian.co.uk/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear>.

WikiLeaks a publicat unul dintre primele rapoarte despre efectele despre care se crede acum că sunt un rezultat al Stuxnet – accidentul de la centrala nucleară de la Natanz, în Iran. Vezi „Serious nuclear accident may lay behind Iranian nuke chief’s mystery resignation“, WikiLeaks, 17 iulie 2009: http://wikileaks.org/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief%27s_mystery_resignation.

Dovezile provenind de la compania de spionaj global Stratfor, scurse de WikiLeaks, indică implicarea israeliană. Vezi „E-mail ID 185945, The Global Intelligence Files“: http://wikileaks.org/gifiles/docs/185945_re-alpha-s3-g3-israel-iran-barak-hails-munitions-blast-in.html (toate linkurile au fost accesate în data de 16 octombrie 2012).

36. „Pentesting“, prescurtarea de la „penetration testing“ [teste de penetrare] este un termen din ingineria de securitate care desemnează organizarea legală, autorizată a unui atac împotriva unui sistem informatic sau împotriva unei rețele de computere, așa cum ar face-o un utilizator neautorizat, pentru a evalua cât este aceasta de sigură. Cercetătorii în materie de securitate sunt recrutați deseori din comunitatea de hackeri pentru a face teste de penetrare pe sisteme sigure.
37. Prinde Steagul este la origine un joc jucat afară, în aer liber, în care de obicei două echipe trebuie să apere o bază și să păzească un steag. Obiectivul este să prindă steagul celeilalte echipe și să se întoarcă cu el la bază. La conferințele de hackeri se joacă o versiune computerizată, unde echipele atacă și apără sisteme și rețele informatice.
38. Cupa Sysadmin este o prescurtare de la System Administrator Cup. Un administrator de sistem este o persoană care lucrează în domeniul IT și întreține sau operează un sistem sau o rețea informatică. Jacob vrea să spună că exercițiul era ca un turneu pentru administratori de sistem.
39. „Aaron spune că criptarea protejează confidențialitatea, comerțul“, USIS Washington File, 13 octombrie 1998: http://www.fas.org/irp/news/1998/10/98101306_clt.html (accesat în data de 21 octombrie 2012).
40. Site-ul Acordului de la Wassenaar: <http://www.wassenaar.org> (accesat în data de 21 octombrie 2012).
41. Andy se referă la diverse evenimente ale „Primului Război Criptografic“ al anilor '90. Când activiștii cypherpunk au început să răspândească instrumente puternice de criptografiere cum ar fi software-ul liber, administrația SUA a luat măsuri pentru a împiedica utilizarea cu succes a instrumentelor

criptografice. A numit criptografia muniție și i-a restricționat exportul; a încercat să introducă tehnologii concurente care erau stricate în mod intenționat, în așa fel încât reprezentanții legii să poată descifra informațiile; și a încercat să introducă controversata schemă „key escrow”. O scurtă vreme după trecerea în noul secol s-a crezut în general că acele eforturi au fost învinse definitiv. Cu toate acestea, acum are loc un „Al Doilea Război Criptografic”, împreună cu eforturi legislative și tehnice de a sabota sau marginaliza folosirea criptografiei.

42. Exemplul de calcul a fost făcut pentru cele 196,4 miliarde de minute de apeluri de pe fix efectuate în Germania în 2010, digitalizate cu un codec audio de 8 Kbps, care însumau o cantitate de 11 784 Petabiți (Pb), rotunjiți (cu tot cu consumul suplimentar) la 15 Pb. Presupunând costuri aproximative de stocare de 500 000 USD (500 kUSD) pentru un Pb, ajungem la suma de 7,5 milioane USD, sau în jur de 6 milioane EUR. La aceasta se mai adaugă costurile unui echipament informatic decent al centrului de date, costurile puterii de procesare, conexiunilor și ale angajaților. Chiar dacă se includ și cele 101 miliarde de minute de apeluri mobile din Germania, cu încă 50 Pb și 18,3 milioane EUR, prețul rămâne mai mic decât cel al unui avion militar ca Eurofighter (90 de milioane EUR) sau F22 (150 de milioane USD).
43. Pentru mai multe informații despre VASTech vezi site-ul buggedplanet: <http://buggedplanet.info/index.php?title=VASTECH> (accesat în data de 21 octombrie 2012).
44. Scandalul supravegherii domestice fără mandat de către NSA este cel mai important caz de supraveghere în masă din istoria Statelor Unite. Legea Foreign Intelligence Surveillance Act din 1978 (FISA) a declarat ca fiind ilegale acțiunile de spionaj fără mandat ale agențiilor SUA împotriva cetățenilor SUA. După atentatele din 11 septembrie, Agenția Națională de Securitate a început să încalce masiv prevederile FISA, autorizată printr-un ordin executiv secret al lui George W. Bush. Administrația Bush și-a revendicat autoritatea executivă de a face aceste lucruri sub prevederile legislației de urgență votate în 2001 de Congres: The Authorization for the Use of Military Force (AUMF) [Autorizația pentru Folosirea Forței Militare] și PATRIOT ACT. Programul de spionaj fără mandat al NSA – care implica cooperarea din partea unor firme private, cum ar fi AT&T – a rămas secret până în 2005, când a fost denunțat de New York Times. Vezi „*Bush Lets U.S. Spy on Callers Without Courts*”, *New York Times*, 16 decembrie 2005: <http://www.nytimes.com/2005/12/16/politics/16pro-gram.html?pagewanted=all>.

Unii reporteri ai *New York Times* fuseseră contactați anonim de cineva care scursese informații despre existența programului de supraveghere fără mandat. În 2004, Bill Keller, director executiv al *New York Times* la vremea aceea, a acceptat, la cererea administrației Bush, să nu publice știrea timp de un an, până când Bush va fi fost ales din nou. În 2005, *New York Times* s-a grăbit să publice articolul când a aflat că administrația ar fi pe cale să elaboreze un ordin de restricție, cum fusese cel din cazul Pentagon Papers. Administrația Bush a negat că ar fi fost comisă vreo ilegalitate în programul NSA. Departamentul de Justiție a lansat imediat o anchetă pentru a găsi sursa scurgerii, care a implicat douăzeci și cinci de agenți federali și cinci procurori. Unii membri din conducerea Partidului Republican au cerut urmărirea în justiție a publicației *New York Times* sub prevederile Legii Spionajului.

Ca urmare a publicării articolului în *New York Times*, alte denunțuri au apărut în presă, alcătuind treptat imaginea nelegiurii și a risipei la cele mai înalte niveluri ale NSA. Grupări militante ca American Civil Liberties Union (ACLU) și Electronic Frontier Foundation (EFF) au intentat o serie de procese în instanță. Într-unul dintre aceste procese, ACLU *versus* NSA, reclamanților le-a fost negată plângerea din cauză că nu puteau dovedi că fuseseră spionați personal. Într-un alt proces, Hepting *versus* AT&T, Mark Klein, un angajat al AT&T, a adus în instanță un affidavit care dezvăluia dimensiunile cooperării dintre AT&T și programul de spionare domestică. Vezi secțiunea destinată companiei AT&T de pe site-ul EFF: <https://www.eff.org/cases/hepting>.

Mark Klein a fost martor în cazul Hepting *versus* AT&T. Ca fost angajat al AT&T, care lucrase în Folsom, San Francisco, declarația sa, făcută organizației EFF în cazul Hepting *versus* AT&T, a scos la iveală existența „Camelei 641A”, o instalație de interceptare strategică operată de AT&T pentru NSA. Instalația permitea accesul la conducte de fibră optică ce conțineau rețeaua principală a traficului de internet, oferind capacitatea de a supraveghea tot traficul de internet care intra și ieșea din clădire, atât cel extern, cât și cel intern. Alt informator împotriva NSA, William Binney, a estimat că există până la 20 de astfel de instalații, toate plasate în puncte strategice în rețeaua de telecomunicații a Statelor Unite.

Declarația lui Klein oferă informații importante despre programul de supraveghere al NSA, confirmat de alți informatori împotriva NSA. Acesta este un exemplu de „interceptare strategică” – tot traficul de internet care trece prin Statele Unite este copiat și stocat pe o perioadă nelimitată. Se poate ști cu certitudine că traficul domestic al SUA este de asemenea

interceptat și stocat pentru că, din punctul de vedere al tehnologiei, când se lucrează cu un trafic de un asemenea volum, este imposibil să se trieze traficul pentru care ar fi necesar un mandat FISA. Interpretarea oficială a legii FISA afirmă acum că a avut loc o „interceptare” doar atunci când o comunicație domestică deja interceptată și stocată de către NSA este „accesată” în baza de date a NSA, și că doar în acest caz este necesar un mandat. Cetățenii SUA ar trebui să plece de la premisa că tot traficul telecomunicațiilor (inclusiv apelurile telefonice, mesajele SMS, e-mailurile și navigarea pe internet) este monitorizat și stocat pentru totdeauna în centrele de date ale NSA.

În 2008, ca reacție la numărul mare de litigii rezultat din scandalul acesta, Congresul SUA a aprobat o serie de amendamente la legea FISA din 1978 care au fost semnate imediat de președinte. Acestea au creat temeiul pentru acordarea unei „imunități retroactive” foarte controversate împotriva urmăririi în justiție pentru încălcarea FISA. În timpul campaniei sale prezidențiale, senatorul Barack Obama făcuse din „transparență” o parte importantă a programului său și a promis să protejeze denunțătorii, dar când a venit la putere în 2009, Departamentul de Justiție a continuat politicile administrației Bush, ieșind într-un final victorios în cazul Hepting, dar și în altele, prin acordarea „imunității retroactive” companiei AT&T.

Deși investigația Departamentului de Justiție pentru a găsi sursa primului articol al *New York Times* a eșuat în ceea ce privește găsirea informatorului anonim, ea a dus la găsirea altora, care ieșiseră la lumină după apariția articolului. Unul dintre ei era Thomas Drake, fost angajat al NSA într-o funcție de conducere executivă, care reclamase ani de zile Comisiei Congresionale pentru Monitorizarea Spionajului corupția și risipa din programul „Trailblazer” condus de NSA. Reclamațiile interne au fost înăbușite, după cum au fost și toți funcționarii statului care doreau să continue cercetările în privința lor. După articolul din *New York Times*, Drake dezvăluise situația programului Trailblazer ziarului *Baltimore Sun*. El a fost pus sub acuzație în urma unei investigații a Marelui Juriu, desemnat drept „inamic al statului” și condamnat sub prevederile Legii Spionajului. Vezi „The Secret Sharer”, *New Yorker*, 23 mai 2011: http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_ma-yer?currentPage=all.

Urmărirea penală a lui Drake s-a prăbușit în urma unei intense examinări publice care a avut loc în iunie 2011, iar după diverse încercări eșuate de a-l obliga pe Drake să accepte o înțelegere cu procurorul, Departamentul de Justiție s-a mulțumit cu pledoaria sa de vinovăție referitoare la o abatere minoră. Drake a primit un an cu suspendare.

Efectul negativ al scandalului supravegherii NSA continuă. Organizația ACLU se află în litigiu pentru a contesta constituționalitatea amendamentelor FISA din 2008 în procesul *Amnesty et. al. versus Clapper*. Vezi „FISA Amendment Act Challenge”, ACLU, 24 septembrie 2012: <http://www.aclu.org/national-security/amnesty-et-al-v-clapper>.

În cazul *Jewel versus NSA*, EFF încearcă să pună capăt supravegherii fără mandat a NSA. Procesul a fost respins în 2009 după ce administrația Obama și-a susținut imunitatea în virtutea unor secrete de stat. Vezi pagina EFF despre procesul *Jewel versus NSA*: <https://www.eff.org/cases/jewel>. Totuși, Curtea de Apel pentru cel De-al Nouălea Circuit a permis redeschiderea cazului în decembrie 2011. Thomas Drake și alți informatori împotriva NSA, William Binney și J. Kirk, depun mărturie în cazul *Jewel versus NSA*. Administrația Obama – care și-a făcut campanie cu un program pentru transparență – a urmărit penal mai mulți denunțatori sub prevederile Legii Spionajului decât toate celelalte administrații luate împreună. (Toate linkurile din această notă au fost accesate în data de 23 octombrie 2012.)

45. Vezi pagina despre sistemul Eagle pe buggedplanet.info/in-dex.php?title=AMESYS#Strategic_28.22Massive.22.29_Applications (accesat în data de 22 octombrie 2012).
46. „Istanța judecătorească germană ordonă ștergerea datelor telecomunicațiilor stocate”, BBC, 2 martie 2010: <http://news.bbc.co.uk/1/hi/world/europe/8545772.stm> (accesat în data de 15 octombrie 2012).
47. Directiva 2006/24/EC a Parlamentului și Consiliului European cere statelor europene să rețină datele telecomunicațiilor cetățenilor lor pe o perioadă între șase și douăzeci și patru de luni. Aplicarea acestei directive în Germania a fost declarată neconstituțională. În mai 2012, Comisia EU a intentat un proces la Curtea Europeană de Justiție în cazul Germaniei pentru că nu s-a conformat directivei (vezi publicația de presă a Comisiei: http://europa.eu/rapid/press-release_IP-12-530_en.htm, accesată în data de 15 octombrie 2012).
48. Vezi „Suedia aprobă legea monitorizării telecomunicațiilor”, BBC, 19 iunie 2008: <http://news.bbc.co.uk/1/hi/world/europe/7463333.stm>. Pentru mai multe informații despre FRA-lagen, vezi Wikipedia: http://en.wikipedia.org/wiki/FRA_law (ambele linkuri au fost accesate în data de 10 octombrie 2012).
49. Metadatele sunt „date despre date”. În contextul acestei discuții, metadatele se referă la alte date decât „conținutul” comunicării electronice. Este aspectul exterior al plicului, nu conținutul său. Supravegherea metadelor nu vizează conținutul e-mailurilor, ci mai degrabă toate informațiile

din jurul conținutului – cui a fost trimis e-mailul sau de către cine, adresa IP (deci locația) de unde a fost trimis, ora și data fiecărui e-mail etc. Ideea este însă că tehnologia pentru interceptarea metadatelor este aceeași cu tehnologia pentru interceptarea conținutului. Dacă acorzi cuiva dreptul să-ți supravegheze metadatele, echipamentul lor trebuie să intercepteze și conținutul comunicațiilor tale. În afară de acest lucru, majoritatea persoanelor nu înțeleg că „metadatele luate ca întreg înseamnă conținut” – când toate metadatele sunt puse la un loc se produce o imagine extrem de detaliată a comunicațiilor cuiva.

50. Amesys face parte din gruparea Bull, care făcea cândva concurență Dehomag-ului, o filială a IBM, în ceea ce privește vânzarea sistemelor cu cartele perforate naziștilor. Vezi Edwin Black, *IBM and the Holocaust* (Crown Books, 2001). Pentru mai multe informații despre spionarea de către Gaddafi a cetățenilor libanezi din Regatul Unit folosind echipament de supraveghere Amesys, vezi „Exclusive: How Gaddafi Spied on the Fathers of the New Libya”, OWNLeu, 1 decembrie 2011: <http://owni.eu/2011/12/01/exclusive-how-gaddafi-spied-on-the-fathers-of-the-new-libya> (accesat în data de 22 octombrie 2012).
51. WikiLeaks a început să publice în decembrie 2011 „The Spy Files”, dezvăluind dimensiunile supravegherii în masă. Acestea pot fi accesate la <http://wikileaks.org/the-spyfiles.html>.
52. Pentru mai multe detalii vezi buggedplanet: <http://buggedplanet.info/index.php?title=LY>
53. Congresul Chaos Communication este întâlnirea anuală a comunității internaționale a hackerilor, organizată de Chaos Computer Club.
54. Jacob se referă la ZTE, unul din cei doi producători chinezi de bunuri electronice (celălalt fiind Huawei) care sunt suspectați de multă lume că ar fi vulnerabile la accesarea datelor lor de către cineva neautorizat. Jacob sugerează că infrastructura de comunicații primită „cadou” are un cost – faptul că va fi, prin însăși alcătuirea sa, susceptibilă supravegherii chineze.
55. Kill Your Television este numele unei forme de protest împotriva comunicațiilor în masă, în cadrul căreia oamenii evitau televizorul în favoarea activităților sociale.
56. „Efectul de rețea” este efectul pe care-l are faptul că o persoană efectuează o anumită activitate asupra probabilității ca și alte persoane să efectueze aceeași activitate.
57. Pentru mai multe informații despre investigația Marelui Juriu, vezi „Notă despre diversele încercări de a persecuta WikiLeaks și pe cei asociați ei” care precedă discuția.

58. Conform publicației *Wall Street Journal*: „Conform unor documente analizate de *Wall Street Journal*, guvernul SUA a obținut un tip controversat de hotărâre judecătorească secretă prin care compania Google Inc. și micul furnizor de internet Sonic.net Inc. erau obligate să predea informații din conturile de e-mail ale voluntarului WikiLeaks Jacob Appelbaum [...] Procesul WikiLeaks a devenit un banc de probă pentru interpretarea legii în prima parte a anului acestuia, când Twitter a atacat în instanță o hotărâre judecătorească de a preda arhivele conturilor mai multor susținători WikiLeaks, inclusiv ale d-lui Appelbaum [...] Ordinul căuta adresele „internet protocol” sau IP ale dispozitivelor de pe care persoanele vizate se conectau la conturile lor. O adresă IP este un număr unic acordat unui aparat conectat la internet. Hotărârea cerea și adresele de e-mail ale persoanelor care comunicau cu aceste conturi. Hotărârea a fost emisă sub sigiliu, dar Twitter a primit din partea curții dreptul de a notifica abonații ale căror informații erau căutate [...] Hotărârile judecătorești care au fost analizate de *Wall Street Journal* vizează același tip de informații cu cele pe care Twitter a fost somat să le predea. Hotărârea secretă pentru compania Google datează din 4 ianuarie și cere uriașului motor de căutare să predea adresa IP de pe care dl Appelbaum s-a conectat la contul său gmail.com și adresele de e-mail și adresele IP ale utilizatorilor cu care a comunicat începând cu data de 1 noiembrie 2009. Nu este clar dacă Google a atacat în instanță hotărârea sau a predat documentele cerute. Hotărârea secretă pentru compania Sonic este datată 15 aprilie și cere lui Sonic să predea același tip de informație despre contul de e-mail al dlui Appelbaum începând cu data de 1 noiembrie 2009. În 31 august, curtea a permis ca sigiliul să fie ridicat de pe hotărârea Sonic și să trimită dlui Appelbaum o copie”.
- „Ordine secrete vizează e-mailurile”, *Wall Street Journal*, 9 octombrie 2011: <http://online.wsj.com/article/SB10001424052970203476804576613284007315072.html> (accesat în data de 11 octombrie 2012). Pentru mai multe detalii, vezi „Notă despre diversele încercări de a persecuta WikiLeaks și pe cei asociați ei” care precedă discuția.
59. „WikiLeaks cere companiilor Google și Facebook să desigileze citațiile US”, *Guardian*, 8 ianuarie 2011: <http://www.guardian.co.uk/media/2011/jan/08/wikileaks-calls-google-facebook-us-subpoenas> (accesat în data de 16 octombrie 2012). Pentru mai multe detalii, vezi „Notă despre diversele încercări de a persecuta WikiLeaks și pe cei asociați ei” care precedă discuția.
60. Vezi „Notă despre diversele încercări de a persecuta WikiLeaks și pe cei asociați ei” care precedă discuția.

61. Pentru mai multe detalii, vezi site-ul Europe *versus* Facebook: http://www.europe-v-facebook.org/EN/Data_Pool/data_pool.html (accesat în data de 24 octombrie 2012).
 62. O Scrisoare de Siguranță Națională sau SSN [„National Security Letter”, NSL] este o scrisoare trimisă de o agenție SUA prin care se cer „date fără conținut” sau „metadate”, cum ar fi arhive ale tranzacțiilor financiare, registre IP sau adrese de contact din e-mail. Oricine primește o SSN trebuie să predea informația cerută, altminteri va suferi urmări penale. O SSN nu are nevoie de autorizația unui tribunal, poate fi emisă direct de o agenție federală. Din acest motiv este similară așa-numitei „somații administrative” – un ordin în vederea predării de informații care are nevoie doar de monitorizare administrativă, nu și juridică. Din acest motiv, se poate spune că SSN-urile încalcă protejările împotriva percheziției și confiscării arbitrare ale Celui De-al Patrulea Amendament. SSN-urile conțin și o clauză de păstrare forțată a tăcerii, ceea ce înseamnă că este o infracțiune ca cineva care primește o SSN să vorbească despre ea cu altcineva. Din acest motiv, se poate spune că SSN-urile încalcă libertatea de expresie garantată de Primul Amendament. În procesul *Doe versus Gonzales*, clauza de păstrare forțată a tăcerii a fost declarată neconstituțională. Legea a fost schimbată pentru a acorda celor care primesc o SSN dreptul să o conteste în instanță, lucru care a satisfăcut Curtea pentru cel De-al Doilea Circuit că folosirea lor nu mai este neconstituțională. SSN-urile continuă să fie criticate de activiștii pentru libertățile civice și contestate în instanță.
- Folosirea SSN-urilor a crescut în mod drastic după ce a fost aprobată legea PATRIOT Act în 2001. De obicei, cei care primesc SSN-uri sunt furnizori de servicii, cum e cazul ISP-urilor sau instituțiilor financiare. Arhivele cerute sunt în mod normal ale clienților celui care primește SSN-ul. Acesta nu poate informa clientul că arhivele sale au fost cerute. Deși cei care primesc SSN-uri au dreptul de a le contesta în instanță, clauza de păstrare forțată a tăcerii îl împiedică pe cel vizat să afle măcar de existența SSN-ului, așa-dar îl împiedică să o conteste în instanță. Pentru a înțelege cât de dificil de justificat este acest lucru, vezi o filmare a avocatului general adjunct al FBI încercând să răspundă la întrebarea lui Jacob Appelbaum, „Cum pot să mă duc la un judecător dacă partea terță e obligată să păstreze tăcerea și nu poate să-mi spună că sunt vizat de către voi?” Răspunsul ei îți dă fiori: „Există unele momente când lucrurile astea sunt necesare”: <http://youtu.be/dTuxoLDnmJU> (poate fi găsit de asemenea, împreună cu material contextual, la Privacy SOS: <http://privacysos.org/node/727>).

Conform Electronic Frontier Foundation, „Dintre toate puterile periculoase de supraveghere ale guvernului care au fost dezvoltate de USA PATRIOT Act, puterea pe care o are Scrisoarea de Siguranță Națională (SSN) după prevederile 18 U.S.C. § 2709, după cum a fost dezvăluit în Secțiunea 505 a legii PATRIOT, este una dintre cele mai înspăimântătoare și invazive. Aceste scrisori, trimise furnizorilor de servicii de comunicații precum companiile de telefonie și ISP-urile, permit FBI-ului să ceară în secret date despre comunicațiile private și activitatea de internet a oricăror cetățeni americani, fără nici o monitorizare semnificativă sau vreo analiză premergătoare a unui organ juridic. Cei care primesc SSN-uri sunt supuși unui ordin care le interzice să dezvăluie existența scrisorii colegilor de muncă, prietenilor sau măcar membrilor familiei, cu atât mai puțin publicului.” Vezi: <https://www.eff.org/issues/national-security-letters>. Vezi de asemenea colecția de documente referitoare la Scrisoarea de Siguranță Națională a Electronic Frontier Foundation, publicate sub prevederile Legii Libertății Informației: <https://www.eff.org/issues/foia/07656JDB> (toate linkurile din această notă au fost accesate în data de 23 octombrie 2012).

63. Vezi mai sus, nota 41, despre „Primul Război Criptografic” al anilor ’90.
64. Julian se referă la SSL/TLS, care este un algoritm criptografic încorporat acum ca standard în fiecare browser și care este folosit pentru navigare secretă – de exemplu, când browser-ul este folosit pentru tranzacții financiare pe internet.
65. Pentru unul din multele exemple, vezi „Blackberry, Twitter probed in London riots”, Bloomberg, 9 august 2011: <http://www.bloomberg.com/news/2011-08-09/blackberry-messages-probed-in-u-k-rioting-as-police-say-looting-organized.html> (accesat în data de 16 octombrie 2012).
66. De exemplu, un membru al grupării LulzSec, care a scos la iveală puncte slabe ale practicilor de securitate ale Sony publicând date personale ale clienților Sony, a fost arestat după ce i-a fost aflată identitatea de pe site-ul proxy HideMyAss.com în urma unei hotărâri judecătorești în SUA. Vezi „Lulzsec hacker pleads guilty over Sony attack”, BBC, 15 octombrie 2012: <http://www.bbc.com/news/technology-19949624> (accesat în data de 15 octombrie 2012).
67. SOPA se referă la Stop Online Piracy Act (Legea Opririi Pirateriei Online). PIPA se referă la Protect Intellectual Property Act (Legea pentru Protecția Drepturilor de Proprietate Intelectuală). Ambele sunt legi propuse în SUA care au căpătat o importanță mondială în 2012. Ambele sunt expresii legislative clare ale dorinței industriei de conținut, reprezentată de Recording Industry Association of America [Asociația Industriei de Înregistrări din

America], de a promulga în întreaga lume intrarea în vigoare a legilor proprietății intelectuale, iar asta într-o manieră cât se poate de dură, ca reacție la distribuția gratuită online de produse culturale. Ambele legi propuneau să se garanteze agențiilor executive ale SUA puterea absolută și universală de a cenzura internetul, ceea ce amenința să „rupă internetul”. Ambele au fost primite cu indignare de către părți substanțiale ale comunității internaționale online și au provocat o reacție puternică din partea actorilor industriali ale căror interese se bazează pe un internet liber și deschis.

La începutul lui 2012, Reddit, Wikipedia și alte câteva mii de site-uri și-au închis serviciile în semn de protest împotriva acestor legi, instigând la grele presiuni publice asupra reprezentanților publici. Alți furnizori de servicii online, cum ar fi Google, au încurajat petițiile. În consecință, ambele legi au fost suspendate până la reconsiderarea și discutarea faptului dacă reprezintă cea mai bună abordare a problemei proprietății intelectuale în domeniul online. Episodul este văzut ca prima descoperire semnificativă și afirmare a puterii eficiente de lobby deținute asupra Congresului de către industria internetului.

68. Vezi „Notă despre diversele încercări de a persecuta WikiLeaks și pe cei asociați ei” care precedă discuția.
69. ACTA se referă la Anti-Counterfeiting Trade Agreement [Acordul Comercial de Combateră a Contrafacerii]. Este un tratat multilateral internațional, negociat în secret timp de mai mulți ani, condus de către Statele Unite și Japonia, care instituie, în parte, obligații noi și aspre în vederea protejării proprietății intelectuale.

Unele ciorne inițiale ale ACTA au fost dezvăluite publicului în 2008, după ce au fost scurse către WikiLeaks, provocând exclamații generale de dezaprobare din partea activiștilor pentru cultura liberă și a susținătorilor online. Vezi secțiunea ACTA de pe WikiLeaks: <http://wikileaks.org/wiki/Category:ACTA>.

Telegramele diplomatice ale SUA distribuite de către WikiLeaks organizației La Quadrature Du Net la începutul lui 2011 au arătat că ACTA a fost negociată în secret în mod explicit pentru a se accelera crearea unor reguli extreme de sancționare a IP-urilor, care ar putea apoi fi impuse cu forța unor țări mai sărace care au fost excluse din acord. Vezi „WikiLeaks Cables Shine Light on ACTA History”, La Quadrature Du Net, 3 februarie 2011: <http://www.laquadrature.net/en/wikileaks-cables-shine-light-on-acta-history> (accesat în data de 23 octombrie 2012).

În iulie 2012, după o campanie condusă de site-ul La Quadrature Du Net și Jérémie Zimmermann, ACTA a fost învinsă în Parlamentul European.

70. M.A.I.D. (Mutually) Assured Information Destruction [Distrugere de Informații Asigurată Reciproc] este „un program care furnizează servicii de «key escrow» cu acționare de la distanță, temporizator și autentificare verificabilă și opțiunea de codificare de urgență. Distruge automat cifrele criptografice după ce este depășit un prag temporal configurabil de către utilizator”: <https://www.noise-bridge.net/wiki/M.A.I.D.>
Unele legi, ca Regulation of Investigatory Powers Act [Legea Reglementării Puterilor de Investigare] din 2000, sau RIPA, fac ca Regatul Unit să fie un regim destul de ostil criptografiei. Sub legea RIPA, indivizii pot fi obligați să descifreze date sau să predea parola la ordinul unui ofițer al poliției. Nu e necesară monitorizarea de către un organ judecătoresc. Refuzul poate conduce la acuzații de infracționalitate. Într-un proces, dacă acuzatul/acuzata pretinde că a uitat parola, are loc o inversare a sarcinii de a aduce dovezi. Pentru a evita să fie condamnat(ă), acuzatul/acuzata trebuie să dovedească că a uitat parola. Lucrul acesta, spun criticii legii, constituie o prezumție de vinovăție. Prin comparație, deși au avut loc multe litigii referitoare la aceleași probleme și în Statele Unite, iar situația e departe de a fi ideală, în circumstanțe similare au fost raportate mai multe succese prin invocarea Primului sau a Celui De-al Patrulea Amendament. Vezi articolul „Freedom from Suspicion, Surveillance Reform for a Digital Age”, publicat de JUSTICE, 4 noiembrie 2011, disponibil la: <http://www.justice.org.uk/re-sources.php/305/freedom-from-suspicion>.
Pentru mai multe informații despre sistemul de fișiere Rubberhose, vezi „The Idiot Savants’ Guide to Rubberhose”, Suelette Dreyfus: <http://marutukku.org/current/src/doc/maruguide/t1.html> (toate linkurile au fost accesate în data de 24 octombrie 2012).
71. O arhivă a vechii liste de e-mailuri Cypherpunk poate fi descărcată la: <http://cryptome.org/cpunks/cpunks-92-98.zip>.
Tim May a fost membru fondator al listei de e-mailuri Cypherpunk. Vezi *Cyphernomicon*-ul său, un FAQ despre istoria și filosofia cypherpunk: <http://www.cypherpunks.to/faq/cypher-nomicron/cyphernomicon.html> (ambele linkuri au fost accesate în data de 24 octombrie 2012).
72. „*Proposed US ACTA plurilateral intellectual property trade agreement (2007)*”, WikiLeaks, 22 mai 2008: http://wikileaks.org/wiki/Proposed_US_ACTA_multilateral_intellectual_property_trade_agreement_%282007%29 (accesat în data de 21 octombrie 2012).
73. „*Massive Takedown of Anti-Scientology Videos on YouTube*”, Electronic Frontier Foundation, 5 septembrie 2008: <https://www.eff.org/deeplinks/2008/09/massive-takedown-anti-scientology-videos-youtube> (accesat în data de 16 octombrie 2012).

74. „EU-India Free Trade Agreement draft, 24 Feb 2009”, WikiLeaks, 23 iunie 2009: http://wikileaks.org/wiki/EU-India_Free_Trade_Agreement_draft,24_Feb_2009 (accesat în data de 21 octombrie 2012).
75. Peer-to-peer, sau P2P, se referă la o rețea în care fiecare computer poate funcționa în calitate de client sau de server pentru toate celelalte (fiecare computer poate atât să trimită, cât și să primească informație), permițând distribuirea rapidă a unor conținuturi de date cum ar fi muzică, înregistrări video sau orice fel de informație digitală.
76. Cloud computing se referă la o situație în care multe dintre funcțiile îndeplinite în mod normal de un computer, cum ar fi stocarea de date (inclusiv datele de utilizator pentru diverse aplicații), găzduirea și administrarea de software și furnizarea și procesarea energiei cu care funcționează software-ul, se face la distanță, departe de computerul ca atare, „în nor” [*cloud* se traduce prin *nor*] – de regulă de către companii care oferă servicii de cloud computing prin internet. În loc să aibă nevoie de un computer complet, tot ceea ce îi trebuie utilizatorului este un aparat care poate accesa internetul, iar restul este servit utilizatorului prin internet. Metafora „în nor” ascunde faptul că toate datele și metadatele utilizatorului se află de fapt într-un computer undeva într-un centru de date, cel mai probabil controlat de o companie mare, cum ar fi Amazon, și în timp ce utilizatorii nu mai au controlul complet asupra lor, îl are altcineva.
77. Vezi „Notă despre diversele încercări de a persecuta WikiLeaks și pe cei asociați ei” care precedă discuția.
78. DIASPORA este o rețea de socializare care permite fiecărui utilizator să funcționeze ca propriul său server prin instalarea software-ului DIASPO-RA, care îi permite să păstreze controlul asupra datelor sale. A fost creat ca o alternativă la Facebook care permite confidențialitatea. Este nonprofit și este deținut de utilizator: <http://diasporaproject.org>.
79. Primul Napster (1999–2001) a fost un serviciu inovativ de tipul peer-to-peer pentru distribuția de muzică. A avut o popularitate enormă, dar a fost închis repede prin acțiuni juridice intentate de Asociația Industriei de Înregistrări din America din cauza încălcării drepturilor de autor. După faliment, numele Napster a fost cumpărat și folosit pentru un alt magazin online de vânzare de muzică.
80. Vezi „Notă despre diversele încercări de a persecuta WikiLeaks și pe cei asociați ei” care precedă discuția.
81. Benjamin Bayart este președintele companiei French Data Network, cel mai vechi ISP activ din Franța și un susținător al neutralității internetului și al software-ului liber. Vezi pagina sa de Wikipedia (în franceză):

http://fr.wikipedia.org/wiki/Benjamin_Bayart (accesată în data de 15 octombrie 2012).

82. Larry Lessig este un academician și activist american cunoscut mai cu seamă pentru viziunile sale despre drepturile de autor și cultura liberă. Blogul său se află la: <http://lessig.tumblr.com> (accesat în data de 15 octombrie 2012).
83. Există multe informații fascinante referitoare la această chestiune în telegramele diplomatice ale SUA publicate de WikiLeaks. Pentru o discuție interesantă, vezi următoarele telegrame (după ID-ul de referință al telegramei, toate linkurile au fost accesate în data de 24 octombrie 2012):
07BEIRUT1301: <http://wikileaks.org/cable/2007/08/07BEIRUT1301.html>
08BEIRUT490: <http://wikileaks.org/cable/2008/04/08BEIRUT490.html>
08BEIRUT505: <http://wikileaks.org/cable/2008/04/08BEIRUT505.html>
08BEIRUT523: <http://wikileaks.org/cable/2008/04/08BEIRUT523.html>.
84. Vezi ID-ul de referință al telegramei 10MOSCOW228, WikiLeaks: <http://wikileaks.org/cable/2010/02/10MOSCOW228.html> (accesat în data de 24 octombrie 2012).
85. Pentru mai multe informații despre uciderea fără proces a cetățenilor americani Anwar al-Awlaki și a fiului său, Abdulrahman al-Awlaki, vezi Glenn Greenwald, „The due-process-free assassination of U.S. citizens is now reality”, Salon, 30 septembrie 2011: http://www.salon.com/2011/09/30/awlaki_6. Și „The killing of Awlaki's 16-year-old son”, Salon, 20 octombrie 2011: http://www.salon.com/2011/10/20/the_killing_of_awlakis_16_year_old_son.
„Este pur și simplu imposibil să ne imaginăm o desconsiderare mai violentă a mecanismelor fundamentale ale republicii decât dezvoltarea unei agenții a ramurii executive, secrete, care nu poate fi deloc trasă la răspundere și care colectează în același timp informații despre toți cetățenii și apoi aplică o „matrice de dispoziție” pentru a determina ce pedeapsă trebuie să se stabilească. Aceasta este clasică distopie politică adusă la realitate” – Glenn Greenwald, „Obama moves to make the War on Terror permanent”, *Guardian*, 24 octombrie 2012: <http://www.guardian.co.uk/commentisfree/2012/oct/24/obama-terrorism-kill-list> (toate linkurile au fost accesate în data de 24 octombrie 2012).
86. Pentru informații ulterioare, vă rugăm să consultați „The Anonymity Bibliography, Selected Papers in Anonymity”, ediție îngrijită de Roger Dingledine și Nick Mathewson: <http://freehaven.net/anonbib> (accesat în data de 24 octombrie 2012).

Moneda chaumiană este emisă central, dar folosește criptografia pentru a asigura tranzacții anonime. Moneda chaumiană se deosebește de Bitcoin,

altă monedă electronică discutată pe larg mai jos, în cazul căreia toate tranzacțiile sunt publice, dar moneda nu are o autoritate centrală.

87. Pentru mai multe informații despre blocada bancară împotriva WikiLeaks, vezi „Notă despre diversele încercări de a persecuta WikiLeaks și pe cei asociați ei” care precedă discuția.
88. Julian se referă aici la planurile Regatului Unit de a crește folosirea dispozitivelor electronice de urmărire. Vezi „Over 100,000 offenders to be electronically tagged”, *Guardian*, 25 martie 2012: <http://www.guardian.co.uk/society/2012/mar/25/prisons-and-probation-criminal-justice> (accesat în data de 22 octombrie 2012).

În momentul discuției, Julian se afla în arest la domiciliu, în așteptarea rezultatului procesului său de extrădare. După închiderea sa în izolare, fără acuzare, în decembrie 2010, detenția lui Julian a fost transformată în arest domiciliu după ce a plătit o sumă de 300 000 de lire sterline pentru eliberarea pe cauțiune. O condiție a eliberării sale a fost consemnarea la o anumită adresă într-un anumit interval temporar, iar acest regim a fost impus de un dispozitiv electronic de urmărire fixat în jurul gleznei sale, administrat de o firmă privată de securitate contractată de guvernul Regatului Unit. Mișcările lui Julian erau controlate în așa măsură încât era constrâns să raporteze zilnic poliției, la o anumită oră, timp de peste 550 de zile. În momentul publicării celor de față, Julian se află consemnat la Ambasada Ecuadorului din Londra, care este înconjurată în fiecare moment de Poliția Metropolitană a Londrei. În iunie 2012, Julian a intrat în ambasadă căutând azil politic din cauza persecuției Statelor Unite și a aliaților săi. A primit azil în august 2012.

89. „Is CCA Trying to Take Over the World?”, American Civil Liberties Union, 21 februarie 2012: <http://www.aclu.org/blog/prisoners-rights/ccatrying-take-over-world>.
„Passing House Bill will worsen already pressing civil rights issue”, ANNARBOR.com, 2 august 2012: <http://annarbor.com/news/opinion/passing-house-bill-will-worsen-already-pressing-civil-rights-issue>.
Vezi, de asemenea, „Goldman Sachs to invest \$9.6m in New York inmate rehabilitation”, *Guardian*, 2 august 2012: <http://www.guardian.co.uk/society/2012/aug/02/goldman-sachs-invest-new-york-jail> (toate linkurile au fost accesate în data de 24 octombrie 2012).

90. Bitcoin (<http://bitcoin.org>) este prima implementare care a avut succes a unui concept clasic al mișcării cypherpunk: moneda digitală criptografică. Moneda Bitcoin este discutată pe larg mai jos, dar o explicație introductivă excelentă despre tehnologia și filosofia din spatele ei poate fi găsită la

„Understanding Bitcoin“, Al Jazeera, 9 iunie 2012: <http://www.aljazeera.com/indepth/opinion/2012/05/20125309437931677.html> (accesat la data de 22 octombrie 2012).

91. E-gold a fost o monedă electronică și o afacere care a început în 1996. Proprietarii au fost acuzați de Departamentul de Justiție al SUA de „complot pentru spălare de bani“. Au pledat vinovați și au primit pedepse cu suspendare, arest domiciliu și muncă în favoarea comunității. Judecătorul care a dat sentința a spus că meritau sentințe ușoare din cauză că nu intenționaseră să facă activități ilegale. Vezi „Bullion and Bandits: The Improbable Rise and Fall of E-Gold“, *Wired*, 9 iunie 2009: <http://www.wired.com/threatlevel/2009/06/e-gold> (accesat în data de 22 octombrie 2012).
92. Înaintea internetului, rețeaua X.25 era cea mai mare rețea globală pentru schimbul de date, existând în paralel cu rețeaua de telefonie. Contorizarea pe X.25 se baza pe cantitatea de date trimise și primite, nu pe lungimea unei conexiuni, ca în cazul rețelei de telefonie. Porțile de acces (așa-numitele PADs) permiteau conectarea la rețeaua X.25 de la o rețea de telefonie prin intermediul unui modem sau al unor cuplaje acustice. Pentru mai multe detalii vezi Wikipedia: <http://en.wikipedia.org/wiki/X.25> (accesat în data de 24 octombrie 2012).
93. David Chaum este criptograf și inventator de protocoale criptografice. Este un pionier al tehnologiilor monetare digitale și a elaborat eCash, una dintre primele monede electronice criptate și anonime.
94. Pentru a vedea efectul pe care l-au avut recenziile negative din presă vezi, „Bitcoin implodes, falls more than 90 percent from June peak“, *arstechnica*, 18 octombrie 2011: <http://arstechnica.com/techpolicy/2011/10/bitcoin-implodes-down-more-than-90-percent-from-june-peak> (accesat în data de 22 octombrie 2012).
95. Vezi, de exemplu, „The Underground Website Where You Can Buy Any Drug Imaginable“, *Gawker*, 1 iunie 2011: <http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable> (accesat în data de 22 octombrie 2012).
96. În ultimii ani, Lawrence Lessig a adăugat activității sale timpurii din domeniul copyrightului și al culturii (care poate fi văzută, de pildă, în cartea sa *Free Culture*, 2004) un interes față de procesul de corupere a democrației americane prin intermediul lobby-ului congressional. Vezi The Lessig Wiki: <http://wiki.lessig.org>.
97. Asociația Correctional Peace Officers din California este un grup de interese din California care face, în mod curent, donații de câte șapte cifre în timpul alegerilor statale, deși nu este, an de an, cea mai mare donatoare de

campanie. Vezi „California reelin“, *The Economist*, 17 martie 2011: <http://www.economist.com/node/18359882>. Și „The Golden State's Iron Bars“, Reason, iulie 2011: <http://reason.com/archives/2011/06/23/the-golden-states-iron-bars>. Vezi și pagina Asociației Correctional Peace Officers din California pe site-ul FollowTheMoney al National Institute for Money in State Politics: <http://www.followthemoney.org/database/topcontributor.phtml?u=3286&y=0> (toate linkurile au fost accesate în data de 22 octombrie 2012).

98. Hanz von Foerster (1911–2002) a fost un cercetător american de origine austriacă și arhitect al ciberneticii. Așa-numitul său „imperativ etic“ sau motto era: „Acționează tot timpul în așa fel încât să sporești numărul opțiunilor“ sau, în germană: „Handle stets so, daß die Anzahl der Wahlmöglichkeiten größer wird“.
99. Jacob atribuie această observație lui John Gilmore. [În text, *And everybody else who is struggling to get along isn't acknowledged as even having bits that are worth flipping in the first place.* – n.tr.]
100. Pentru mai multe informații despre hărțuirea lui Jacob și a altor persoane asociate cu WikiLeaks, vezi „Notă despre diversele încercări de a persecuta WikiLeaks și pe cei asociați ei“ care precedă discuția.
101. Isaac Mao este un blogger, creator de software și investitor din China. Este cofondator al site-ului CNBlog.org și membru al consiliului de conducere al Proiectului Tor.
102. Vezi pagina de WikiLeaks despre Nadhmi Auchi: http://wikileaks.org/wiki/Nadhmi_Auchi (accesat în data de 24 octombrie 2012).
103. Articolele pot fi găsite pe site-ul WikiLeaks, aici: http://wikileaks.org/wiki/Eight_stories_on_Obama_linked_billionaire_Nadhmi_Auchi_censored_from_the_Guardian,_Observer,_Telegraph_and_New_Statesman (accesat în data de 24 octombrie 2012).
104. În linii mari, atât <http://cables.mrkva.eu/>, cât și <http://cablegatesearch.net> furnizează modalități excelente de a compara versiunile revizuite și pe cele complete ale telegramelor, pentru a vedea ce au eliminat partenerii media ai WikiLeaks.
105. „Qaddafi's Son Is Bisexual and Other Things the *New York Times* Doesn't Want You to Know“, *Gawker*, 16 septembrie 2011: <http://gawker.com/5840809/qaddafis-son-is-bisexual-and-other-things-the-new-york-times-doesnt-want-you-to-know-about>. Exemplul citat se referă la ID-ul de referință al telegramei 06TRIPOLI198, WikiLeaks: <https://wikileaks.org/cable/2006/05/06TRIPOLI198.html>.

Părțile redactate pot fi urmărite pe site-ul Cablegatesearch, care arată arhiva revizuirilor, redactările fiind subliniate în roz: <http://www.cablegate-search.net/cable.php?id=06TRIPOLI198&version=1291757400> (toate linkurile au fost accesate în data de 22 octombrie 2012).

106. Pentru telegrama originală vezi telegrama cu ID-ul de referință 10STATE17263, la WikiLeaks: <http://wikileaks.org/cable/2010/02/10STATE17263.html>.

Pentru articolul din *New York Times*, vezi „Iran Fortifies Its Arsenal With the Aid of North Korea”, *New York Times*, 29 noiembrie 2010: http://www.nytimes.com/2010/11/29/world/middle-east/29missiles.html?_r=0.

Acceași telegramă a fost folosită de către David Leigh de la *The Guardian* pentru articolul său: „WikiLeaks cables expose Pakistan nuclear fears”, *Guardian*, 30 noiembrie 2010: <http://www.guardian.co.uk/world/2010/nov/30/wikileaks-cables-pakistan-nuclear-fears>. Versiunea revizuită a telegramei, publicată de *The Guardian*, fără un număr de referință, e redusă la doar două paragrafe referitoare la Pakistan. „US embassy cables: XXXXXXXXXXXXXXX”, *Guardian*, 30 noiembrie 2010: <http://www.guardian.co.uk/world/us-embassy-cables-documents/250573>.

Pe site-ul Cablegatesearch se poate vedea în ce măsură textul a fost revizuit, aici găsim arhiva revizuirilor, părțile redactate ale documentului fiind aproape în întregime subliniate în roz: <http://www.cablegate-search.net/cable.php?id=10STATE17263&version=1291486260> (toate linkurile au fost accesate în data de 22 octombrie 2012).

107. Pentru telegrama originală vezi telegrama cu ID-ul de referință 08KYIV2414, la site-ul WikiLeaks: <http://wikileaks.org/cable/2008/12/08KYIV2414.html>.

Pentru versiunea redactată de *The Guardian*, vezi „US embassy cables: Gas supplies linked to Russian mafia”, 1 decembrie 2010: <http://www.guardian.co.uk/world/us-embassy-cables-documents/182121?INTCMP=SRCH>.

Editările pot fi urmărite pe site-ul Cablegatesearch, care arată arhiva revizuirilor, editările fiind subliniate în roz: <http://www.cablegatesearch.net/cable.php?id=08KYIV2414&version=1291255260> (toate linkurile au fost accesate în data de 22 octombrie 2012).

108. Pentru telegrama originală vezi telegrama cu ID-ul de referință 10ASTANA72, la WikiLeaks: <http://wikileaks.org/cable/2010/01/10ASTANA72.html>.

Pentru versiunea redactată de *The Guardian*, vezi „US embassy cables: Kazakhstan - the big four”, *Guardian*, 29 noiembrie 2010: <http://www.guardian.co.uk/world/us-embassy-cables-documents/245167?INTCMP=SRCH>.

Editările pot fi urmărite pe site-ul Cablegatesearch, care arată arhiva revizuirilor, redactările fiind subliniate în roz: <http://www.cablegatesearch.net/cable.php?id=10ASTANA72&version=1291113360> (toate linkurile au fost accesate în data de 22 octombrie 2012).

109. Vezi, de pildă, telegrama cu ID-ul de referință 09TRIPOLI413, despre companiile europene de energie cu sedii în Libia. Reprezentarea grafică de pe site-ul Cablegatesearch, care pune în roz editările făcute de *The Guardian*, arată că publicația a scos toate referirile făcute la numele companiilor energetice sau la directorii acestora, în afară de cele privitoare la Gazprom, compania rusească de energie. Deși o parte din conținut este oarecum justificator pentru companiile europene, redactările sunt minuțioase, iar versiunea redactată prezintă o imagine complet diferită: <http://www.cablegate-search.net/cable.php?id=09TRIPOLI413&version=1296509820> (accesat în data de 22 octombrie 2012).

110. Telegrama originală menționată în acest exemplu conținea 5 226 de cuvinte. Versiunea editată publicată în *The Guardian* conținea doar 1 406 de cuvinte. Pentru telegrama originală vezi telegrama cu ID-ul de referință 05SO-FIA1207, pe site-ul WikiLeaks: <http://wikileaks.org/cable/2005/07/05SOFIA1207.html>.

Pentru versiunea editată de *The Guardian*, vezi „US embassy cables: Organised crime in Bulgaria“, 1 decembrie 2010: <http://www.guardian.co.uk/world/us-embassy-cables-documents/36013>.

Pentru articolul din *The Guardian* bazat pe această telegramă, vezi „WikiLeaks cables: Russian government «using mafia for its dirty work»“, *Guardian*, 1 decembrie 2010: <http://www.guardian.co.uk/world/2010/dec/01/wikileaks-cable-spain-russian-mafia>.

Pe site-ul Cablegatesearch se poate vedea în ce măsură textul a fost revizuit, aici găsindu-se arhiva revizuirilor, editările fiind subliniate în roz: <http://www.cablegatesearch.net/cable.php?id=05SOFIA1207&version=1291757400>.

Exemplul bulgar este discutat de publicația *Bivol*, partener media al WikiLeaks, în „Unedited cable from Sofia shows the total invasion of the state by organized crime (Update: Cable Comparison)“, WL Central, 18 martie 2011: <http://wlcentral.org/node/1480>.

De asemenea, vezi „The Guardian: Redacting, censoring or lying?“, WL Central, 19 martie 2012: <http://wlcentral.org/node/1490>.

Interesant, pe subiectul celor două articole ale WL Central, este comentariul jurnalistului David Leigh de la *The Guardian* și răspunsurile la acesta. (Toate linkurile au fost accesate în data de 22 octombrie 2012.)

111. Exemplul acesta se referă la telegrama cu ID-ul de referință 09BERLIN1108. Editările pot fi urmărite pe site-ul Cablegatesearch, care arată arhiva revizuirilor, editările fiind subliniate în roz: <http://www.cablegate-search.net/cable.php?id=09BERLIN1108&cversion=1291380660> (accesat la data de 22 octombrie 2012).
112. Pentru mai multe exemple, vezi site-ul cabledrum: www.cabledrum.net/pages/censorship.php
113. „Interceptarea telecomunicațiilor. Președinția a furnizat informații despre situația actuală [...] A atras atenția în legătură cu reacția negativă pe care chestiunea a primit-o din partea mass-media [...] În aceste circumstanțe, președinția a recunoscut că progresul în această chestiune este foarte lent [...] Mai multe delegații și-au exprimat reținerea în ceea ce privește pregătirea unei declarații de presă, atrăgând atenția că acest lucru ar putea provoca o reacție în lanț și o continuare a reacției negative în mass-media. Deși a declarat că nu și-a schimbat poziția, comisia a informat delegațiile că un mod de a ieși din impas ar fi să urmeze o strategie similară cu cea urmată în abordarea chestiunii pornografiei infantile pe internet. Deși acesta a fost un subiect diferit, el are și tangențe cu chestiunea interceptării” – „European Commission, Police Co-operation Working Group meeting on interception of telecommunications”, 13–14 octombrie 1999. Vezi documentul complet la adresa: http://www.quintessenz.at/doqs/000100002292/1999_10_13,-Police%20Cooperation%20Working%20Group%20mixed%20committee%20meeting.pdf (accesat la data de 24 octombrie 2012).
114. Vezi „Notă despre diversele încercări de a persecuta WikiLeaks și pe cei asociați ei” care precedă discuția.
115. Jacob se referă la procesul *Gilmore versus Gonzales*, nr. 435 F.3d 1125 (al 9-lea Cir. 2006). John Gilmore, unul dintre primii cypherpunks, a ajuns cu un proces până la Curtea Supremă a SUA pentru a scoate la iveală conținutul unei legi secrete – o directivă de securitate – ce restricționa dreptul cetățenilor de a călători cu avionul fără a se legitima. Pe lângă atacarea constituționalității unei astfel de prevederi, Gilmore ataca faptul că prevederea ca atare este secretă și nu putea fi dezvăluită, deși are efecte constrângătoare asupra cetățenilor SUA. Curtea a consultat în secret directiva de securitate și a decis împotriva lui Gilmore în privința constituționalității directivei. Cu toate acestea, conținutul legii nu a fost niciodată dezvăluit pe perioada deliberărilor. Vezi *Gilmore versus Gonzales* la PapersPlease.org: <http://papersplease.org/gilmore/facts.html> (accesat în data de 22 octombrie 2012).
116. Christiania este o zonă autodeclarată, care se autoguvernează în Copenhaga, Danemarca. Fostă cazarmă militară, a fost ocupată în anii

1970 de o comunitate colectivist/anarhistă. Și-a creat un statut juridic unic în Danemarca.

117. Principiul neutralității rețelei implică împiedicarea ISP-urilor (prin lege, se cere de obicei) de a restricționa accesul utilizatorilor lor la rețelele care participă la internet, inclusiv restricționarea conținutului. Vezi pagina Fundației Electronic Frontier despre subiectul neutralității rețelei: <https://www.eff.org/issues/net-neutrality> (accesat în data de 24 octombrie 2012).
118. „Blocking WikiLeaks e-mails trips up Bradley Manning prosecution“, Politico, 15 martie 2012: <http://www.politico.com/blogs/under-the-radar/2012/03/blocking-wikileaks-emails-trips-up-bradley-man-ning-117573.html> (accesat în data de 21 octombrie 2012).
119. Pentru mai multe informații despre Wau Holland, vezi Wau Holland Stiftung: <http://www.wauland.de>
120. „Stasi still in charge of Stasi files“, WikiLeaks, 4 octombrie 2007: http://www.wikileaks.org/wiki/Stasi_still_in_charge_of_Stasi_files (accesat în data de 22 octombrie 2012).
121. „Iată ce puteți face ca să schimbați lumea, chiar acum, pentru a o face mai bună. Luați toți banii pe care-i cheltuim pe armament și apărare în fiecare an și cheltuiți-i în loc pe hrănirea, îmbrăcarea și educarea săracilor lumii acesteia, lucru pe care [banii, n.tr.] l-ar face de mai multe ori, fără să excludă un singur om, și am putea explora spațiul, împreună, atât cel cunoscut, cât și cel necunoscut, pentru totdeauna, în pace“ – Bill Hicks. Pentru a viziona înregistrarea video, vezi „Bill Hicks—Positive Drugs Story“: <http://youtu.be/vX1CvW38cHA> (accesat la data de 24 octombrie 2012).
122. Legea Sarbanes-Oxley din 2002 este o lege aprobată în SUA ca răspuns la scandalurile corporatiste și de contabilitate ale Enron, Tyco International, Adelphia, Peregrine Systems și WorldCom. Legea urmărește eliminarea practicilor corupte care au dus la aceste crize. Paragraful 1107 al acestei legi, codificat USC 1513(e), stabilește ca infracțiune orice încercare de a sancționa denunțatorii.
123. Evgeny Morozov (2011), *The Net Delusion: The Dark Side of Internet Freedom*, Public Affairs.
124. Pentru informații despre software-ul liber, vezi „The Free Software Definition“, pe site-ul sistemului de operare GNU: <https://www.gnu.org/philosophy/free-sw.html>.

Hardware cu sursă deschisă înseamnă un tip de hardware care nu este îngreunat de brevete de proprietate, care este construit la standarde libere, unde nu există legi împotriva ingineriei inverse sau a manipulării (nu există legi de tipul „anti-sustragere“) și unde principiile concepției, instrucțiunile

și planul sunt accesibile, astfel încât oricine le are și are resursele necesare în acest sens să poată crea un duplicat.

Pentru mai multe informații despre hardware-ul cu sursă deschisă, vezi „Exceptionally Hard and Soft Meeting: exploring the frontiers of open source and DIY“, EHSM: <http://ehsm.eu>. Vezi și „Open-source hardware“ pe Wikipedia: https://en.wikipedia.org/wiki/Open-source_hardware (toate linkurile au fost accesate în data de 24 octombrie 2012).

125. Vezi filmarea introductivă despre imprimanta 3D RepRap, care funcționează pe principiul hardware-ului liber și cu sursă deschisă: <http://vimeo.com/5202148> (accesat în data de 24 octombrie 2012).
126. Fraza „Be the trouble you want to see in the world“ [„Fii tulburarea pe care vrei să o vezi în lume“] este preluată din „A Softer World“, o publicație fotografică online comică: <http://www.asofterworld.com/index.php?id=189> (accesat în data de 24 octombrie 2012).
127. Pentru a studia mai departe oricare dintre problemele ridicate în timpul conversației, Jacob recomandă următoarele două resurse bibliografice: „The Anonymity Bibliography, Selected Papers in Anonymity“, ediție îngrijită de Roger Dingledine și Nick Mathewson: <http://freehaven.net/anonbib>. „The Censorship Bibliography, Selected Papers in Censorship“, ediție îngrijită de Philipp Winter: www.cs.kau.se/philwint/censorbib (ambele linkuri au fost accesate în data de 24 octombrie 2012).
128. Această notă este lăsată intenționat goală.
129. Nawaat.org este un blog colectiv independent, lansat în 2004, în Tunisia: <http://nawaat.org/portail>. Tunileaks a fost lansat de către Nawaat în luna noiembrie a anului 2010, cu publicarea unor telegrame referitoare la Tunisia, preluate de la WikiLeaks: <https://tunileaks.appspot.com>. Pentru mai multe informații despre Tunileaks și despre eforturile guvernului Ben-Ali împotriva sa, vezi „Tunisia: Censorship Continues as Wikileaks Cables Make the Rounds“, Global Voices Advocacy, 7 decembrie 2010: <http://advocacy.globalvoicesonline.org/2010/12/07/tunisia-censorship-continues-as-wikileaks-cables-make-the-rounds> (toate linkurile au fost accesate în data de 24 octombrie 2012).



Viața cetății este într-o dinamică complexă, iar pentru o bună funcționare a acesteia e nevoie de cetățeni bine informați. *Polis* aduce laolaltă cele mai bune cărți de științe politice și sociale, care configurează modele societale viabile și repere pentru toți cei interesați de bunul mers al societății în care trăiesc.

Cristian Pîrvulescu

O explicație clară a modului în care controlul exercitat de către corporații și guverne asupra internetului reprezintă o amenințare la adresa libertății noastre și a democrației.

Oliver Stone

Apeluri telefonice, SMS-uri, chat-uri, căutări pe Google, fotografiile pe Facebook: ne comunicăm în fiecare clipă informațiile personale privind locurile în care suntem, opiniile, obiceiurile, fricile sau gândurile noastre, fără a ne face griji privitor la ce se va întâmpla cu acestea. Dar se pare că internetul, gândit ca un formidabil mijloc de emancipare, e pe cale să devină cel mai eficient instrument de control imaginat vreodată. Toate aceste informații pe care cu atâta ușurință le împărtășim sunt înregistrate, stocate și pot fi cu ușurință analizate și exploatare de către agenții de spionaj extrem de complexe și de aliații lor reprezentați de corporații transnaționale. Aceasta este teama lui Julian Assange și a prietenilor lui, gânditori și activiști rebeli din prima linie a bătăliei pentru cyberspațiu, care militează pentru un internet liber. Discuția lor ne deschide ochii asupra amenințărilor actuale la adresa libertăților noastre politice și individuale.

JULIAN ASSANGE este redactorul-șef al WikiLeaks, distins cu premiul „Noile Media” al Amnesty International (2009), premiul fundației Sydney pentru pace (2011), premiul „Walkley” pentru jurnalism (2011) și premiul „Martha Gellhorn” (2011). Este creatorul a numeroase proiecte de software inspirate de filosofia cypherpunk, inclusiv al sistemului de fișiere Rubberhose pentru criptare și al codului original pentru WikiLeaks. A mai publicat cartea *Underground* (împreună cu Suelette Dreyfus, 2012), o istorie a mișcării internaționale a hackerilor.

Tradiție din 1989



www.litera.ro

ISBN 978-606-33-0610-5



9 786063 306105